日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１１日

出願番号
Application Number: 特願２００２－２９８３０９

[ST. 10/C]: [ＪＰ２００２－２９８３０９]

出願人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００３年 ９月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号 出証特２００３－３０７９２５４

【書類名】　特許願

【整理番号】　0290539802

【提出日】　平成14年10月11日

【あて先】　特許庁長官殿

【国際特許分類】　E05B 49/00

G08B 23/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　油井　康二

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　松村　広幸

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　八重樫　章

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代理人】

【識別番号】　100091546

【弁理士】

【氏名又は名称】　佐藤　正美

【電話番号】　03-5386-1775

【手数料の表示】

【予納台帳番号】　048851

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9710846

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子鍵装置およびドアロック制御システム

【特許請求の範囲】

【請求項１】

生体情報を取得する生体情報取得手段と、

前記生体情報が記憶されている生体情報記憶部と、

電子鍵情報が記憶されている電子鍵情報記憶部と、

前記電子鍵情報を外部に送信する機能を備える通信手段と、

前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、

前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する制御手段と、

を備えることを特徴とする電子鍵装置。

【請求項２】

前記生体情報取得手段は、前記生体情報として指紋情報を取得するものであることを特徴とする請求項１に記載の電子鍵装置。

【請求項３】

前記生体情報取得手段は、前記生体情報として虹彩情報を取得するものであることを特徴とする請求項１に記載の電子鍵装置。

【請求項４】

前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であることを特徴とする請求項１に記載の電子鍵装置。

【請求項５】

電子鍵情報を記憶する電子鍵装置と、前記電子鍵装置からの前記電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置とからなるドアロック制御システムであって、

前記電子鍵装置は、

生体情報を取得する生体情報取得手段と、

前記生体情報が記憶されている生体情報記憶部と、

電子鍵情報が記憶されている第１の電子鍵情報記憶部と、

前記電子鍵情報を外部に送信する機能を備える第１の通信手段と、

前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、

前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する第１の制御手段と、

を備え、

前記制御装置は、

電子鍵情報を記憶する電子鍵装置からの前記電子鍵情報の受信を行なうための第２の通信手段と、

電子鍵情報を記憶する第２の電子鍵情報記憶部と、

前記第２の通信手段を通じて前記電子鍵装置から受信した前記電子鍵情報と、前記第２の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて前記ドアロック機構を制御する第２の制御手段と、

を備えることを特徴とするドアロック制御システム。

【請求項６】

請求項５に記載のドアロック制御システムにおいて、

前記電子鍵装置の前記生体情報取得手段は、前記生体情報として指紋情報を取得するものであることを特徴とするドアロック制御システム。

【請求項７】

請求項５に記載のドアロック制御システムにおいて、

前記電子鍵装置の前記生体情報取得手段は、前記生体情報として虹彩情報を取得するものであることを特徴とするドアロック制御システム。

【請求項８】

請求項５に記載のドアロック制御システムにおいて、

前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であり、

前記制御装置は、前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする個人情報を記憶する個人情報記憶部を備えるとともに、前記電子鍵装置

から受信した前記電子鍵情報と、前記第２の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前記ドアからの入退出を管理する手段を備える

ことを特徴とするドアロック制御システム。

【請求項９】

請求項５に記載のドアロック制御システムにおいて、

前記電子鍵情報は、前記制御装置ごとに、同一のものが存在しないように一元管理されて割り振られた識別情報である

ことを特徴とするドアロック制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ドアの施錠、開錠を制御するための電子鍵情報を外部に送出する機能を有する電子鍵装置および当該電子鍵装置と通信を行なって前記電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロック制御システムに関する。

【０００２】

【従来の技術】

最近、従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロック制御システムを玄関ドアなどに採用している住戸等においては、鍵シリンダー機構に精通しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

【０００３】

そこで、このような鍵シリンダー機構を用いない電子鍵によるドアロック制御システムが注目されている。例えば、この電子鍵によるドアロックシステムの一例として、親機は、予め登録されている電子鍵情報としてのＩＤコードと、電子鍵情報としての子機から受信したＩＤコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献１（特開平９－４２９３号公報参照））。

【０００４】

【特許文献１】

特開平９－４２９３号公報。

【０００５】

【発明が解決しようとする課題】

ところで、鍵を紛失した場合には、ドアロック機構の鍵シリンダーを当該鍵以外の鍵を用いるものに交換しない限り、悪意の紛失鍵の拾得者にドアが開錠されてしまうおそれがつきまとう。電子鍵によるドアロックシステムにおいても、電子鍵情報が書き込まれている装置（以下、電子鍵装置と称する）を紛失してしまった場合には、上述した悪意の紛失鍵の拾得者に対抗する対策が必要である。

【０００６】

この発明は、紛失しても、容易に悪意の紛失鍵の拾得者に対抗することができる電子鍵装置および当該電子鍵装置を用いるドアロック制御システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、請求項１の発明による電子鍵装置は、

生体情報を取得する生体情報取得手段と、

前記生体情報が記憶されている生体情報記憶部と、

電子鍵情報が記憶されている電子鍵情報記憶部と、

前記電子鍵情報を外部に送信する機能を備える通信手段と、

前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、

前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する制御手段と、

を備えることを特徴とする。

【０００８】

請求項１の発明による電子鍵装置においては、予め登録された所有者の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができる

ので、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【０００９】

そして、請求項４の発明のように、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報を用いた場合には、個人の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができるので、電子鍵情報は、個人識別情報として使用することができる。

【００１０】

また、請求項５の発明によるドアロック制御システムは、

電子鍵情報を記憶する電子鍵装置と、前記電子鍵装置からの前記電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置とからなるドアロック制御システムであって、

前記電子鍵装置は、

生体情報を取得する生体情報取得手段と、

前記生体情報が記憶されている生体情報記憶部と、

電子鍵情報が記憶されている第１の電子鍵情報記憶部と、

前記電子鍵情報を外部に送信する機能を備える第１の通信手段と、

前記生体情報取得手段で取得された生体情報と、前記生体情報記憶部に記憶されている生体情報とを比較する比較手段と、

前記比較手段での比較結果に基づいて、前記電子鍵情報記憶部の前記電子鍵情報の前記通信手段を通じた送出を制御する第１の制御手段と、

を備え、

前記制御装置は、

電子鍵情報を記憶する電子鍵装置からの前記電子鍵情報の受信を行なうための第２の通信手段と、

電子鍵情報を記憶する第２の電子鍵情報記憶部と、

前記第２の通信手段を通じて前記電子鍵装置から受信した前記電子鍵情報と、前記第２の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較

結果に基づいて前記ドアロック機構を制御する第２の制御手段と、

を備えることを特徴とする。

【００１１】

この請求項５の発明によるドアロック制御システムにおいては、電子鍵装置からは、個人の生体情報が確認されたときにのみ、電子鍵情報が送出され、当該電子鍵情報が制御装置で、予め記憶されている電子鍵情報と比較して認証が取られることによりドアロック制御される。

【００１２】

したがって、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【００１３】

また、請求項８の発明は、請求項５に記載のドアロック制御システムにおいて、

前記電子鍵情報は、同一のものが存在しないように一元管理されて割り振られた識別情報であり、

前記制御装置は、前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする個人情報を記憶する個人情報記憶部を備えるとともに、前記電子鍵装置から受信した前記電子鍵情報と、前記第２の電子鍵情報記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前記ドアからの入退出を管理する手段を備える

ことを特徴とする。

【００１４】

この請求項８の発明によるドアロック制御システムによれば、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報が用いられているので、制御装置では、ドアロック制御機構の制御を行なうとともに、電子鍵情報を個人識別情報として使用して、電子鍵装置の使用者毎のドアを通じての入退出を管理することができる。

【００１５】

【発明の実施の形態】

以下、この発明によるドアロック制御システムの実施形態を、図を参照しながら説明する。

【００１６】

以下に説明する例では、家の玄関ドアに、実施形態のドアロック制御システムを設ける。また、この例では、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。

【００１７】

そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバ装置に接続して、全体として、通信システムを構成している。

【００１８】

この場合に、電子鍵装置は、生体情報取得部と、制御用ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）と、通信手段とを備えるもので、種々の形態のものが使用可能である。この例では、この電子鍵装置の具体例としては、ＩＣカードの他、携帯電話端末、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）端末などを用いることもできる。

【００１９】

電子鍵装置に搭載される制御用ＩＣは電子鍵情報用メモリを備え、その電子鍵情報用メモリには、電子鍵情報が格納されている。この電子鍵情報としては、この例では、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ＩＣチップ製造番号が用いられる。

【００２０】

例えば、図１に示すように、１社あるいは複数社のＩＣチップの製造会社１００１において、製造した制御用ＩＣチップ１００２に対して、一元管理された重複のないＩＣチップ製造番号を付与するようにする。ＩＣチップの製造会社１００１が複数社の場合には、例えば、それぞれのＩＣチップ製造会社１００１に、

予め、制御用ＩＣチップ１００２に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用ＩＣチップ１００２のメモリには、互いに異なるＩＣチップ製造番号が識別情報として記憶される。

【００２１】

この制御用ＩＣチップ１００２は、ＩＣカード製造工場（あるいは製造会社）１００３、携帯電話端末製造工場（あるいは製造会社）１００４、ＰＤＡ端末製造工場（あるいは製造会社）１００５などに供給されて、それらの制御用ＩＣチップと通信手段とが搭載されたＩＣカード、携帯電話端末、ＰＤＡ端末などが製造される。

【００２２】

図２は、この実施形態で用いられるＩＣチップ製造番号の一例を説明するための図である。

【００２３】

この例のＩＣチップ製造番号は、３桁のメーカー番号と、３桁のカテゴリーコードと、４桁のシリアル番号とからなる、合計１０桁の番号（記号を含む）で構成される。

【００２４】

なお、識別情報は、ＩＣチップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、ＩＣチップ製造番号と共に、別個にＩＣのメモリに記憶するようにしてもよい。

【００２５】

電子鍵装置の通信手段としては、この例では、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

【００２６】

次に、この実施形態のドアロック制御システムにおいては、玄関ドアには、電

子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、電子鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

【００２７】

以下に説明する例では、電子鍵装置とドアロック装置との間の通信は、電磁誘導を用いた非接触による通信とされており、後述するように、ドアロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

【００２８】

この実施形態では、ドアの施錠、開錠を制御するための電子鍵情報としては、前述したＩＣチップ製造番号からなる識別情報が用いられる。この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようにする。

【００２９】

この実施の形態では、管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

【００３０】

後述するように、この実施形態では、家族構成員のそれぞれは、自分用の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。

【００３１】

以下に説明する例においては、各人に与えられる本鍵装置としては、ドアロッ

ク制御システムの提供会社が提供するＩＣカードとされる。そして、この本鍵装置であるＩＣカードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ装置に、当該ＩＣカードの所有者の電子鍵情報として登録される。

【００３２】

この場合に、この実施形態では、家族構成員の数分だけ、ＩＣカードが前記提供会社から提供され、それらの複数のＩＣカードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。

【００３３】

さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つＩＣカードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子鍵情報を、家族構成員の個人識別情報として用いることが可能である。

【００３４】

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ドアロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

【００３５】

また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、ＩＣ製造番号）を管理サーバ装置に登録することにより、登録可能である。

【００３６】

なお、本鍵情報とバックアップ鍵情報との電子鍵情報の認証についての取り扱

い方法としては、本鍵情報とバックアップ鍵情報とを同等に扱う方法と、認証用としては本鍵情報のみを原則とし、本鍵情報が抹消されたときに、バックアップ鍵情報が登録されていれば、以後は、バックアップ鍵情報を本鍵情報として取り扱うようにする方法とがある。いずれの方法を用いることができるが、できるだけ、認証用としては、少ない方がセキュリティ上は好ましいと考えられるので、この実施形態では、後者の場合を採用するものとしている。

【００３７】

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

【００３８】

このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。

【００３９】

[実施形態のドアロックシステムを含むセキュリティシステムの概要]

図３は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

【００４０】

家の玄関ドア１には、電子鍵装置と通信を行なうドアロック装置２が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置３が設けられ、ドアロック装置２と接続されている。ドアロック装置２と監視制御装置３とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

【００４１】

監視制御装置３は、ドアロック装置２からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることもできる。しかし、この例では、電子鍵情報の認証は、ドアロック装置２自身において行なうよう

にされている。

【００４２】

そして、この例では、室内には、火災発生を検知する火災センサ４と、ガス漏れを検知するガスセンサ５と、窓の戸締りを検知する窓センサ６ａ，６ｂと、テレビ７が設けられ、それぞれ監視制御装置３に接続されている。監視制御装置３とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

【００４３】

また、図３では省略したが、火災センサ４で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ６ａ，６ｂで賊の侵入を検知したときに、その賊を撮影できるような位置には、監視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置３に接続され、監視カメラの撮影画像が監視制御装置３に供給されるようにされる。

【００４４】

監視制御装置３は、また、電話回線８を通じ、通信ネットワーク９を通じてセキュリティシステムの管理会社が運営する管理サーバ装置１０に接続される。この管理サーバ装置１０も、ドアロック装置２からの電子鍵情報を、監視制御装置３を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

【００４５】

通信ネットワーク９は、携帯電話網をも含み、後述するように、監視制御装置３は、異常状態の発生時に、予め登録された携帯電話端末１１ａ，１１ｂに、当該異常状態の発生を知らせることが可能とされている。さらに、通信ネットワーク９は、インターネットを含み、パーソナルコンピュータ１２は、管理サーバ装置１０に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末１１ａ，１１ｂからも、管理サーバ装置１０にアクセスすることが可能とされている。

【００４６】

なお、この実施形態においては、特許請求の範囲における制御装置は、ドアロ

ック装置２の後述するドアロック制御装置と監視制御装置とで構成されるものである。

【００４７】

次に、ドアロック装置２の具体的構成例およびその動作、また、監視制御装置３の具体的構成例およびその動作について、詳細に説明する。なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

【００４８】

[電子鍵装置の構成例]

前述したように、この実施形態においては、電子鍵装置としては、ＩＣカードの他、携帯電話端末やＰＤＡ端末なども用いることができる。しかし、電子鍵装置は、生体情報の取得部と、制御用ＩＣチップと、通信手段とを備える点では共通している。電子鍵装置がＩＣカードである場合の構成例を次に示す。

【００４９】

＜電子鍵装置の第１の例＞

この第１の例の電子鍵装置は、生体情報として、指紋を用いるＩＣカードの場合の例である。図４（Ａ）は、この例のＩＣカード４０Ｆの表面を示し、この表面には、所有者の氏名と、ＩＤ番号が表示されていると共に、指紋読取部４１の指紋読取窓４１Ｗが形成されている。

【００５０】

また、図４（Ｂ）は、ＩＣカード４０Ｆの内部構成例を示しており、ＩＣカード４０Ｆ内には、指紋読取部４１と、後述するドアロック装置２の電子鍵リード／ライト部と通信を行なうための電磁誘導アンテナ４２と、制御用ＩＣ４３と、情報送受信回路部４４が内蔵されている。

【００５１】

指紋読取部４１は、指紋読取窓４１Ｗに置かれた指の指紋を読み取り、その読み取った指紋の情報を制御用ＩＣ４３に送る。制御用ＩＣ４３は、予め登録されて記憶しているＩＣカード４０Ｆの所有者の指紋情報と、読み取った指紋情報とを比較し、一致しているかどうか判別する。

【００５２】

そして、一致していると判別すると、予め制御用ＩＣ４３内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部４４および電磁誘導アンテナ４２を通じて、外部に送出する。記憶している指紋情報と、読み取った指紋情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

【００５３】

図５は、第１の例の場合のＩＣカード４０Ｆの内部ブロック構成を示すものである。ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）４０１に対してシステムバス４０２を介してプログラムやデータが記録されているＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）４０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）４０４と、電子鍵情報となる識別情報が記憶されている識別情報メモリ４０５と、通信履歴メモリ４０６と、送受信インターフェース４０７と、指紋登録メモリ４０８と、指紋読取部インターフェース４０９と、指紋照合部４１０とが接続されている。

【００５４】

識別情報メモリ４０５には、前述したＩＣ製造番号からなる識別情報が記憶されている。なお、このＩＣカード４０の所有者の氏名、住所の他、所有者のその他の必要な個人情報を記憶することもできる。この個人情報は、父親、母親、子供などの区別が可能なように構成される。

【００５５】

通信履歴メモリ４０６には、各所有者が行ったドアロック装置２の後述する電子鍵リード／ライト部との通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むことが可能とされている。なお、これらの履歴情報は、後述するように、ドアロック装置２のメモリや監視制御装置３のメモリにおける家族構成員の各人に対応するエリアにも記憶されるものである。

【００５６】

送受信インターフェース４０７には、電磁誘導アンテナ４１に接続されている

情報送受信回路部４４が接続されている。

【００５７】

指紋登録メモリ４０８には、当該ＩＣカード４０Ｆの所有者の指紋の情報が予め登録されて記憶されている。指紋読取部インターフェース４０９は、指紋読取部４１で読み取った指紋の情報を取り込むためのものである。指紋照合部４１０は、指紋読取部インターフェース４０９を通じて取得した指紋の情報と、指紋登録メモリ４０８から読み出した前記所有者の指紋の情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス４０２に送出する。指紋照合部４１０は、ハードウエアの構成ではなく、ＣＰＵ４０１によるソフトウエアによる構成とすることもできる。

【００５８】

ＣＰＵ４０１は、前述したように、指紋照合部４１０での判定結果に基づき、指紋一致、つまり、指紋照合がＯＫであったときには、識別情報メモリ４０５から読み出した識別情報からなる電子鍵情報を、送受信インターフェース４０７、情報送受信回路４０８および電磁誘導アンテナ４１を通じて送出し、指紋照合部４１０での判定結果が指紋不一致、つまり、指紋照合がＮＧであったときには、電子鍵情報の送出を禁止する。

【００５９】

また、ＣＰＵ４０１は、電磁誘導アンテナ４２にて受信した情報を、情報送受信回路部４０８および送受信インターフェース４０７を通じて取り込み、通信履歴メモリ４０６に書き込んだりする処理も行なう。

【００６０】

図６は、このときのＣＰＵ４０１での処理動作を説明するためのフローチャートである。

【００６１】

ＣＰＵ４０１は、指紋読取部インターフェース４０９を通じた指紋読取部４１からの指紋情報の受信を待ち（ステップＳ１）、指紋情報を受信したと判別したときには、指紋登録メモリ４０８に登録されている所有者の指紋情報を読み出し、指紋照合部４１０において指紋照合を行なわせる（ステップＳ２）。

【００６２】

そして、ＣＰＵ４０１は、指紋照合部４１０からの指紋照合の判定結果が指紋一致であるか否か判別し（ステップＳ３）、指紋不一致で照合がＮＧであったときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

【００６３】

また、ＣＰＵ４０１は、指紋一致で照合がＯＫであったときには、識別情報メモリ４０５から識別情報を読み出して、電子鍵情報として、情報送受信回路部４４および電磁誘導アンテナ４２を通じて送出する（ステップＳ４）。

【００６４】

そして、ＣＰＵ４０１は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップＳ５）、電磁誘導アンテナ４２、情報送受信回路部４４および送受信インターフェース４０７を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ４０６に書き込み（ステップＳ６）、その後、この処理ルーチンを終了する。

【００６５】

ステップＳ５で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、ＣＰＵ４０１は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップＳ７）、所定時間経過していないと判別したときには、ステップＳ４に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップＳ７で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

【００６６】

以上のように、この例の電子鍵装置としてのＩＣカード４０Ｆによれば、予め登録してある所有者の指紋と、使用者の指紋とを照合して、照合がＯＫである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

【００６７】

＜電子鍵装置の第２の例＞

この第２の例の電子鍵装置は、生体情報として、虹彩を用いるＩＣカードの場合の例である。図７（Ａ）は、この例のＩＣカード４０Ｉの表面を示し、この表面には、所有者の氏名と、ＩＤ番号が表示されていると共に、使用者の虹彩を読み取るための手段として、この例では、ＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）カメラ４５が設けられている。

【００６８】

また、図７（Ｂ）は、ＩＣカード４０Ｉの内部構成例を示しており、ＩＣカード４０Ｉ内には、第１の例のＩＣカード４０Ｆと同様に、電磁誘導アンテナ４２と、制御用ＩＣ４３と、情報送受信回路部４４とが内蔵されていると共に、ＣＣＤカメラ４５からの撮像信号を処理して制御用ＩＣ４３に供給するための撮像信号処理回路部４６が内蔵されている。

【００６９】

使用者は、ＣＣＤカメラ４５により自分の目（虹彩）を撮影させる。ＣＣＤカメラ４５は、撮影した使用者の虹彩情報を撮像信号処理回路部４６を通じて取り込み、その取り込んだ虹彩の情報を制御用ＩＣ４３に送る。制御用ＩＣ４３は、予め登録されて記憶されているＩＣカード４０Ｉの所有者の虹彩情報と、取り込んだ虹彩情報とを比較し、一致しているかどうか判別する。

【００７０】

そして、一致していると判別すると、予め制御用ＩＣ４３内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部４４および電磁誘導アンテナ４２を通じて、外部に送出する。記憶している虹彩情報と、取り込んだ虹彩情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

【００７１】

図８は、第２の例の場合のＩＣカード４０Ｉの内部ブロック構成を示すものである。この第２の例においては、図５の第１の例の指紋登録メモリ４０８と、指紋読取部インターフェース４０９と、指紋照合部４１０とに代わって、虹彩情報登録メモリ４１１と、撮像信号インターフェース４１２と、虹彩照合部４１３とが設けられる。撮像信号インターフェース４１２は、ＣＣＤカメラ４５に接続さ

れている。その他の構成は、第１の例の図５と同様である。

【００７２】

虹彩情報登録メモリ４１１には、当該ＩＣカード４０Ｉの所有者の虹彩の情報が予め登録されて記憶されている。撮像信号インターフェース４１２は、撮像信号処理回路部４６からの虹彩情報を取り込むためのものである。虹彩照合部４１３は、撮像信号インターフェース４１２を通じて取り込んだ虹彩情報と、虹彩情報登録メモリ４１１から読み出した前記所有者の虹彩情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス４０２に送出する。虹彩照合部４１３は、ハードウエアの構成ではなく、ＣＰＵ４０１によるソフトウエアによる構成とすることもできる。

【００７３】

ＣＰＵ４０１は、虹彩照合部４１３での判定結果に基づき、虹彩一致、つまり、虹彩照合がＯＫであったときには、識別情報メモリ４０５から読み出した識別情報からなる電子鍵情報を、送受信インターフェース４０７、情報送受信回路４０８および電磁誘導アンテナ４１を通じて送出し、虹彩照合部４１３での判定結果が虹彩不一致、つまり、虹彩照合がＮＧであったときには、電子鍵情報の送出を禁止する。

【００７４】

図９は、このときのＣＰＵ４０１での処理動作を説明するためのフローチャートである。

【００７５】

ＣＰＵ４０１は、撮像信号インターフェース４１２を通じた撮像信号処理回路部４６からの虹彩情報の受信を待ち（ステップＳ１１）、虹彩情報を受信したと判別したときには、虹彩情報登録メモリ４１１に登録されている所有者の虹彩情報を読み出し、虹彩照合部４１３において虹彩照合を行なわせる（ステップＳ１２）。

【００７６】

そして、ＣＰＵ４０１は、虹彩照合部４１３からの虹彩照合の判定結果が虹彩一致であるか否か判別し（ステップＳ１３）、虹彩不一致で照合がＮＧであった

ときには、処理をそのまま終了して、電子鍵情報の送出は行なわない。

【００７７】

また、ＣＰＵ４０１は、虹彩一致で照合がＯＫであったときには、識別情報メモリ４０５から識別情報を読み出して、電子鍵情報として、情報送受信回路部４４および電磁誘導アンテナ４２を通じて送出する（ステップＳ１４）。

【００７８】

そして、ＣＰＵ４０１は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップＳ１５）、電磁誘導アンテナ４２、情報送受信回路部４４および送受信インターフェース４０７を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ４０６に書き込み（ステップＳ１６）、その後、この処理ルーチンを終了する。

【００７９】

ステップＳ１５で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、ＣＰＵ４０１は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップＳ１７）、所定時間経過していないと判別したときには、ステップＳ１４に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップＳ７で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

【００８０】

以上のように、この第２の例の電子鍵装置としてのＩＣカード４０Ｉによれば、予め登録してある所有者の虹彩と、使用者の虹彩とを照合して、照合がＯＫである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

【００８１】

[生体情報の他の例]

以上の例では、生体情報としては、指紋と、虹彩の場合について説明したが、生体情報としては、これに限られるものではない。例えば手の甲の静脈パターンを生体情報として用いることもできる。この場合には、虹彩情報に代えて、所有

者の手の甲の静脈パターンを登録して記憶しておくとともに、ＣＣＤカメラ４５により、手の甲の静脈パターンを撮影して取り込むことにより、第２の例のＩＣカード４０Ｉの構成をそのまま用いることができる。

【００８２】

なお、以上の例に限らず、個人識別が可能な生体情報であって、所定の手段により取得可能なものであれば、どのような生体情報も、利用することができることは勿論である。

【００８３】

［ドアロック装置の構成］

図１０（Ａ）および図１０（Ｂ）は、ドアロック装置２の構成例を説明するための図である。図１０（Ａ）は、家の外側から玄関ドア１のドアロック装置２の取り付け部分近傍を見た図である。また、図１０（Ｂ）は、玄関ドア１のドアロック装置２の取り付け部分近傍を、玄関ドア１の端面側から見た図である。

【００８４】

この例のドアロック装置２においては、玄関ドア１の外側（戸外側）には、電子鍵装置の例としてのＩＣカード４０Ｆや４０Ｉと通信を行なうための外側電子鍵リーダ／ライタ部２１ｅｘと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての外側ＬＥＤ（Ｌｉｇｈｔ Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ；発光ダイオード）２２ｅｘと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための外側スピーカ２３ｅｘと、外側ドアノブ２４ｅｘとが設けられている。

【００８５】

また、玄関ドア１の内側（屋内側）にも、電子鍵装置の例としてのＩＣカード４０Ｆや４０Ｉと通信を行なうための内側電子鍵リーダ／ライタ部２１ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての内側ＬＥＤ２２ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための内側スピーカ２３ｉｎと、内側ドアノブ２４ｉｎとが設けられている。

【００８６】

玄関ドア１には、さらに、玄関ドア係止片２５と、ロック片２６と、ドア開閉センサ２７が設けられている。さらに、玄関ドア１の内側には、ドアロック装置２の動作を制御するためのドアロック制御装置１００が設けられており、電子鍵リーダ／ライタ部２１ｅｘおよび２１ｉｎ、ＬＥＤ２２ｅｘおよび２２ｉｎ、スピーカ２３ｅｘおよび２３ｉｎ、ドア開閉センサ２７および図示を省略したドアロック機構駆動部が、このドアロック制御装置１００に接続されている。

【００８７】

玄関ドア係止片２５は、ドアノブ２４ｅｘあるいはドアノブ２４ｉｎの操作に応じて、玄関ドアの端面１ａに垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア１が施錠されていないときにも、玄関ドア１の端面１ａと対向する壁の端面側に設けられる凹部に勘合して、玄関ドア１を、係止するためのものである。

【００８８】

ロック片２６は、ドアロック機構の一部を構成する部材であり、図１０では図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面１ａに垂直な方向に摺動移動して、玄関ドア１を施錠するときには、図１０のように、玄関ドア１の端面１ａから突出する状態に固定され、玄関ドア１を開錠するときには、玄関ドア１の端面１ａから突出しない状態に固定される。

【００８９】

なお、図示は省略したが、玄関ドア１の端面１ａと対向する壁の端面には、このロック片２６が突出した状態のときに嵌合される凹部が形成されており、ロック片２６が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片２６が玄関ドア１側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

【００９０】

玄関ドア開閉センサ２７は、例えば光学式センサが用いられ、玄関ドア１が開けられたときは外部光を検知することにより、それを検知し、玄関ドア１が閉じられたときには、玄関ドア１の端面１ａが、壁の端面と衝合することにより外部

光が遮断されることを検知することにより、それを検知して、玄関ドア１の開閉を検知する。

【００９１】

[ドアロック制御装置１００の説明]

次に、ドアロック制御装置１００を中心にしたドアロック装置２の電気的な構成例を図１１に示す。なお、以下の説明においては、電子鍵装置としては、指紋照合認証を行なう第１の例のＩＣカード４０Ｆを用いるものとする。

【００９２】

すなわち、ドアロック制御装置１００は、マイクロコンピュータの構成を備えており、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１０１に対してシステムバス１０２を介してプログラムやデータが記録されているＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１０４と、家族構成員の個々についての電子鍵情報となる識別情報（この例では、ＩＣ製造番号）が記憶されている家族情報メモリ１２０と、監視制御装置３と通信を行なうための通信インターフェース１２１とが接続されている。

【００９３】

家族情報メモリ１２０には、後述するように、管理サーバ装置１０に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続き柄、その他の個人情報も、併せて家族情報メモリ１２０に格納するようにしてもよい。この家族情報メモリ１２０への電子鍵情報の登録に関しては、後述する。

【００９４】

また、システムバス１０２には、インターフェース１０５および１０６を介して内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘが接続され、また、内側ＬＥＤ駆動部１０７を介して内側ＬＥＤ２２ｉｎが接続され、外側ＬＥＤ駆動部１０８を介して外側ＬＥＤ２２ｅｘが接続され、さらに、音声出力インターフェース１０９を介して内側スピーカ２３ｉｎが接続さ

れ、音声インターフェース１１０を介して外側スピーカ２３ｅｘが接続される。

【００９５】

さらに、システムバス１０２には、インターフェース１１１を介してドア開閉センサ２７が接続されると共に、ドアロック機構駆動部１１２を介して、ロック片２６を摺動駆動させるドアロック機構２８が接続される。

【００９６】

電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、ＩＣカード４０Ｆ（または４０Ｉ）と通信を行なう通信部を構成する。電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、この例では、電磁誘導アンテナおよび情報送受信部を含む。

【００９７】

この例のドアロック制御装置１００は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの２通りの制御モードを備えている。

【００９８】

オートロックモードは、ドアロック制御装置１００が、電子鍵リード／ライト部２１ｅｘ，２１ｉｎを介してＩＣカード４０Ｆと通信することに基づき玄関ドア１を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いるものとなる。

【００９９】

また、逐次ロックモードは、少なくとも玄関ドア１の外側の電子鍵リード／ライト部２１ｅｘを通じてＩＣカード４０Ｆと通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部２１ｅｘを通じたＩＣカード４０Ｆとの通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

【０１００】

ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置２を取り付ける際に、後述するように、作業者により監視制御装置３を通じて行なわれる。

【０１０１】

ドアロック装置２がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置１００内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置１００は、当該不揮発性メモリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロックモードかを認識するものである。監視制御装置３を通じたドアロック制御モードの設定動作に関しては、後述する。

【０１０２】

なお、ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置３を通じて行なうのではなく、ドアロック装置２に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置２の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置２に行なっておくようにしても良い。また、ドアロック装置２に、ドアロック装置２の設置作業者が操作可能な入力操作手段、例えばディップスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

【０１０３】

[監視制御装置３の外観の説明]

図１２は、室内に設けられるセキュリティシステム用の監視制御装置３の構成を説明するための外観図であり、この監視制御装置３は、例えば赤外線や電波を用いたリモートコマンダ５０によりリモコン制御可能の構成とされている。

【０１０４】

監視制御装置３の筐体３０には、ビデオカメラ３１が組み込まれている。このビデオカメラ３１は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体３０に対して取り付けられて

いる。このビデオカメラ３１は、セキュリティモードがオンとされたときに、監視制御装置３からの指示により撮影を開始するようにされている。

【０１０５】

また、ビデオカメラ３１による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるようにされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ３１による撮影方向の調整を行なっておくことができる。

【０１０６】

そして、筐体３０には、ビデオカメラ３１による撮影対象部を明るく照明するための撮影用ランプ３２が設けられている。また、筐体３０には、例えば遠赤外線を検知することにより人を検知する人感センサ３３が設けられている。監視制御装置３は、後述するように、セキュリティモードオンのときに人感センサ３３で人を検知したときには、賊の侵入であるとして検知し、撮影用ランプ３２をオンにすると共に、所定の通報先に撮影画像を送るようにする。

【０１０７】

筐体３０には、また、マイクロホン３４とスピーカ３５とが設けられている。マイクロホン３４は、賊の声や賊侵入時の室内の臨場音を収音するためのものである。スピーカ３５は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

【０１０８】

筐体３０には、また、電子鍵リード／ライト部３６が設けられる。この電子鍵リード／ライト部３６は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置３は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部３６により、電子鍵装置としてのＩＣカード４０Ｆを読み取らせた後、後述するようにリモートコマンダ５０の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンダ５０の伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになっている。

【０１０９】

この伝言が記録されているかどうかなどを知らせるため等の用途として、筐体３０には、複数個のＬＥＤ３７が設けられている。また、筐体３０には、さらに、リモートコマンダ５０からのリモコン信号の受信部３８が設けられる。

【０１１０】

また、図１２では図示を省略したが、監視制御装置３の背面パネルには、テレビ受像機７のビデオ入力端子に接続される映像出力端子が設けられている。そして、監視制御装置３には、テレビ受像機７の電源のオン・オフなどを制御するためのリモコン送信部３９が設けられている。

【０１１１】

さらに、監視制御装置３は、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂ、さらには、監視カメラを接続するためのセンサハブを備えている。また、図３で説明したように、監視制御装置３は、電話回線を通じて、セキュリティシステムの管理会社が運営する管理サーバ装置１０にアクセスできるように構成されている。

【０１１２】

［監視制御装置３の構成例］

監視制御装置３の内部構成および監視制御装置３と周辺機器との接続状態の構成例を図１３に示す。

【０１１３】

監視制御装置３は、マイクロコンピュータの構成を備えており、ＣＰＵ２０１に対して、システムバス２０２を介して、プログラムやデータが記録されているＲＯＭ２０３と、ワークエリア用ＲＡＭ２０４と、ドアロック制御装置１００の家族情報メモリ１２０と同様に、電子鍵装置としてのＩＣカード４０Ｆまたは４０Ｉを所有する家族全員の電子鍵情報となる識別情報が記憶されている家族情報メモリ２０５と、ドアロック制御装置１００と通信を行なうためのドアロック装置通信インターフェース２０６と、センサハブ２０７と、ビデオカメラ３１の撮影画像およびマイクロホン３４で収音した音声を記憶するための画像・音声メモリ２０８と、電話回線を通じて管理サーバ装置１０等と通信を行なうための通信インターフェース２０９とが接続されている。

【０１１４】

また、システムバス２０２には、カメラインターフェース２１０を介してビデオカメラ３１が、インターフェース２１１を介して撮影用ランプ３２の照明機構３２０が、インターフェース２１２を介して人感センサ３３が、インターフェース２１４を介して電子鍵リード／ライト部３６が、インターフェース２１５を介してリモコン受信部３８が、インターフェース２１６を介してリモコン送信部３９が、音声入力インターフェース２１８を介してマイクロホン３４が、インターフェース２１９を介してＬＥＤ３７が、音声出力インターフェース２２０を介してスピーカ３５が、それぞれ接続されている。さらに、システムバス２０２は、ビデオ信号出力端子からなるテレビインターフェース２１７を介してテレビ受像機７に接続されている。

【０１１５】

家族情報メモリ２０５は、例えばＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）で構成される。

【０１１６】

家族情報メモリ２０５には、ドアロック制御装置１００の家族情報メモリ１２０と同様に、家族構成員のそれぞれについての識別情報と、個人情報とが格納されている。この明細書では、識別情報と個人情報とからなる情報を、個人プロファイル情報と呼ぶことにする。

【０１１７】

後述するように、この例では、家族構成員すべての個人プロファイル情報は、ドアロック装置２および監視制御装置３が設置されたときに、設置管理者が管理サーバ装置１０に初期登録依頼をすることにより、管理サーバ装置１０から送られてきて、監視制御装置３に自動的に登録される。そして、監視制御装置３は、少なくとも個人プロファイル情報のうちの個人識別情報を電子鍵情報として、ドアロック制御装置１００に転送する。ドアロック制御装置１００は、その電子鍵情報を家族情報メモリ１２０に登録する。

【０１１８】

図１４に、一人分の個人プロファイル情報の例を示す。図１４に示すように、

個人プロファイル情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報は、電子鍵情報の役割を有することは前述した通りであり、図１４に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

【０１１９】

図１４の例においては、個人情報としては、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、ＩＰアドレス、趣味／嗜好情報、家の玄関８からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ２０５に記憶される。

【０１２０】

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置３が玄関ドア７を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置１０からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

【０１２１】

さらに、この例では、この家族情報メモリ２０５には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置３では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図１５は、セキュリティレベルと家族構成員の在宅状況との関係を示すテーブルである。また、図１６は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

【０１２２】

図１６に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベルＡ、レベルＢ、レベルＣ、レベルＤまであり、レベルＡにおいては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ３１による監視の全てを行ない、レベルＢでは、ビデオカメラ３１による監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベルＣでは、火災やガス漏れの監視のみを行ない、レベルＤでは、監視を行なわない、という内容である。

【０１２３】

そして、図１５に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベルＤとされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベルＣとされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベルＢとされる。そして、全員が不在である状況では、全ての監視を行なうレベルＡとされる。

【０１２４】

監視制御装置３では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図１５、図１６のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

【０１２５】

図１５のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンダ５０を用いて監視制御装置３に入力設定することにより、設定を変更することできるように構成されている。

【０１２６】

なお、これら図１５、図１６のテーブル情報は、家族情報メモリ２０５ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

【０１２７】

ドアロック装置通信インターフェース２０６は、ドアロック制御装置１００に

接続されている。センサハブ２０７には、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂおよび１個あるいは複数個の監視カメラ１３が接続される。

【０１２８】

画像・音声メモリ２０８は、セキュリティモードがオンであるときに、ビデオカメラ３１で撮影した画像情報と、マイクロホン３４で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ１３用の画像記憶領域も設けられている。

【０１２９】

監視情報領域は、この例では、所定時間、例えば３０秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

【０１３０】

通信インターフェース２０９は、この例では、ルータ６１に接続されている。ルータ６１は、ＡＤＳＬモデム６２、スプリッタ６３を通じて電話回線６５に接続されている。スプリッタ６３には、電話端末６４が接続される。

【０１３１】

[リモートコマンダ５０の説明]

監視制御装置３用のリモートコマンダ５０は、図１２に示すように、セキュリティボタン５１と、オフボタン５２と、伝言記録ボタン５３と、伝言再生ボタン５４と、メニューボタン５５と、上下左右の選択を行なう４個のキーとその中央の決定キーとからなるカーソルボタン５６とを備えて構成されている。

【０１３２】

メニュー項目としては、この例では、管理サーバ装置１０に対する電子鍵情報としての個人ＩＤの登録、ドアロック装置２のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置３のＲＯＭ２０３に格納されている。

【０１３３】

［管理サーバ装置１０の構成］

次に、管理サーバ装置１０の構成例を図１７に示す。管理サーバ装置１０は、コンピュータの構成を備えており、ＣＰＵ３０１に対して、システムバス３０２を介して、プログラムやデータが記録されているＲＯＭ３０３と、ワークエリア用ＲＡＭ３０４と、ドアロック装置管理データベース３０５と、電子鍵登録・紛失履歴メモリ３０６と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース３０７とが接続されている。また、システムバス３０２には、さらに、ホームページ用メモリ３０８と、画像・音声メモリ３０９とが接続されている。

【０１３４】

ドアロック装置管理データベース３０５には、ドアロック装置２および監視制御装置３のシリアル番号、ドアロック装置２および監視制御装置３が設置された住所、電話番号、ＩＰアドレス、ドアロック装置の利用者の氏名、登録された電子鍵情報を個人プロファイル情報など、ドアロック装置２の管理に必要な事項が格納されている。電話番号、ＩＰアドレスは、ドアロック装置２および監視制御装置３の通信ネットワーク９上のアドレス情報である。

【０１３５】

電子鍵登録・紛失履歴メモリ３０６には、各ドアロック装置２ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ３０８には、ホームページの各ページの表示情報が格納されており、ＣＰＵ３０１の指示に従い、必要がページの表示情報が、このメモリ３０８から読み出されて、通信インターフェース３０７を通じて通信ネットワークに送出される。

【０１３６】

画像・音声メモリ３０９は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置１０では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

【０１３７】

次に、以上のような構成の通信システムにおける種々の動作について、以下に説明する。

【０１３８】

[監視制御装置３における伝言記録および伝言再生；図１８]

前述したように、この例の監視制御装置３は、電子鍵装置、この例ではＩＣカード４０Ｆと、リモートコマンダ５０を用いて、特定の家人を指定して、伝言を記録しておくことができる。伝言が監視制御装置３に記録されているときには、ＬＥＤ３７が点灯あるいは点滅して、その旨を知らせるようにしている。

【０１３９】

そして、監視制御装置３に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置としてのＩＣカード４０Ｆを、この電子鍵リード／ライト部３６により読み取らせ、リモートコマンダ５０により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置３は、記録されている伝言を、テレビ受像機７やスピーカ３５を通じて再生するようにするように構成されている。

【０１４０】

図１８は、この伝言記録および再生のための監視制御装置３の処理を説明するためのフローチャートである。この図１８の各ステップＳの処理は、ＣＰＵ２０１がＲＯＭ２０３に記憶されているプログラムにしたがって実行されるものである。

【０１４１】

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分のＩＣカード４０Ｆを電子鍵リード／ライト部３６にかざして、通信を行なうようにする。ＣＰＵ２０１は、電子鍵リード／ライト部３６でＩＣカード４０Ｆと通信が行なわれたか否か判別し（ステップＳ２１）、通信が行われたと判別すると、受信した識別情報により、誰のＩＣカード４０Ｆと通信したかを認識する（ステップＳ２２）。

【０１４２】

次に、リモートコマンダ５０からのリモコン信号の到来を待ち（ステップＳ２

３）、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン５３の操作によるものか否か判別し（ステップＳ２４）、伝言記録ボタン５３の操作によるものであると判別したときには、ＣＰＵ２０１は、伝言記録動作を行なうようにする（ステップＳ３３）。

【０１４３】

この伝言記録動作においては、監視制御装置３は、ビデオカメラ３１で撮影された伝言者の画像情報をカメラインターフェース２１０を介して取り込み、画像・音声メモリ２０８の伝言記録領域に格納すると共に、マイクロホン３４で収音した伝言音声情報（伝言メッセージ）をインターフェース２１８を通じて取り込み、画像・音声メモリ２０８の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置４０から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ２０８に格納される。

【０１４４】

次に、ＣＰＵ２０１は、家族情報メモリ２０８に記憶されている家族の個人プロファイル情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機７の画面に表示する（ステップＳ３４）。このとき、テレビ受像機７に電源が投入されていないときには、リモコン送信部３８を通じて電源をオンにするリモコン信号をテレビ受像機７に供給して、テレビ受像機７に電源を投入しておく。なお、伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

【０１４５】

操作者は、この伝言相手のリストから、リモートコマンダ５０のカーソルキー５６を用いて、伝言相手の選択入力を行ない、カーソルキー５６中の中央の決定キーを押す。監視制御装置３のＣＰＵ２０１は、この伝言相手の選択入力を受信して（ステップＳ３５）、当該伝言相手の情報を、画像・音声メモリ２０８の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する（ステップＳ３６）。そして、伝言が記録されたことを報知するために、１個のＬＥＤ３７を点灯させる（ステップＳ３７）。ＬＥＤ３７は、図１２に示

したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

【０１４６】

また、ステップＳ２４において、リモコン信号が伝言記録ボタン５３の操作によるものではないと判別したときには、伝言再生ボタン５４の操作によるものであるか否か判別する（ステップＳ２５）。伝言再生ボタン５４の操作によるものでないと判別したときには、ＣＰＵ２０１は、当該操作されたボタンに応じた処理を行なう（ステップＳ２６）。

【０１４７】

そして、ステップＳ２５において、伝言再生ボタン５４の操作によるものであると判別したときには、ＣＰＵ２１は、ステップＳ２２で認識した識別情報を検索子として、画像・音声メモリ２０８の伝言記録領域の記憶内容を検索して、ＩＣカード４０Ｆを電子鍵リード／ライト部３６にかざした操作者宛ての伝言があるか否か判別する（ステップＳ２７）。

【０１４８】

そして、ステップＳ２７において、操作者宛ての伝言が無いと判別したときには、ＣＰＵ２０１は、例えば予めＲＯＭ２０３に用意されている「伝言はありません」の文字情報をテレビ受像機７の画面に表示すると共に、スピーカ３５を通じて音声として放音して、操作者に報知する（ステップＳ２８）。

【０１４９】

また、ステップＳ２７において、操作者宛ての伝言が有ると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ２０８から読み出して、テレビ受像機７に表示すると共に、スピーカ３５から放音して再生する（ステップＳ２９）。

【０１５０】

伝言の再生が終了すると、ＣＰＵ２０１は、テレビ受像機７の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「ＹＥＳ」、「ＮＯ」のいずれかをリモートコマンダ５０のカーソルキー５６を用いて選択する。ＣＰＵ２０１は、当該操作者の選択入力から、伝言を消去す

るか否か判別し（ステップＳ３０）、消去すると判別したときには、画像・音声メモリ２０８の対応する画像・音声情報を消去し（ステップＳ３１）、点灯しているＬＥＤ３７の一つを消灯する（ステップＳ３２）。そして、この伝言記録再生処理ルーチンを終了する。

【０１５１】

また、ステップＳ３０で、伝言を消去しないと判別したときには、そのまま、この伝言記録再生処理ルーチンを終了する。

【０１５２】

［ドアロック制御モードの選択設定；図１９、図２０］

前述したように、この実施形態では、監視制御装置３を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、図１９のフローチャートを参照しながら説明する。

【０１５３】

先ず、監視制御装置３のＣＰＵ２０１は、リモコン受信部３８の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップＳ４１）。この例では、この特定のボタン操作としては、通常の使用者が行なわない操作とされており、例えばセキュリティボタン５１とメニューボタン５５との同時操作などとされている。このような特定のボタン操作は、ドアロック装置２の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

【０１５４】

ステップＳ４１で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップＳ４２）。また、ステップＳ４１で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機７の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップＳ４３）。

【０１５５】

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー

項目の選択をリモートコマンダ５０のカーソルキーを用いて行なう。ＣＰＵ２０１は、リモコン受信部３８の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップＳ４４）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップＳ４５）。そして、設定項目の決定操作がなされたか否か判別する（ステップＳ４６）。また、ステップＳ４４で、メニュー項目の選択操作がなされないと判別したときには、即座にステップＳ４６に進んで設定項目の決定操作がなされたか否か判別する。

【０１５６】

ステップＳ４６で、設定項目の決定操作がなされないと判別したときには、ステップＳ４４に戻る。また、ステップＳ４６で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップＳ４７）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップＳ４８）。

【０１５７】

ステップＳ４７で、選択された設定項目はドアロック制御モードの設定であると判別したときには、ＣＰＵ２０１は、テレビ受像機７の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップＳ４９）。操作者は、この選択画面において、いずれかの選択入力をカーソルキー５６を用いて行なう。

【０１５８】

そこで、ＣＰＵ２０１は、リモコン受信部３８を監視して、オートロックモードが選択されたか否か判別し（ステップＳ５０）、オートロックモードが選択されたと判別したときには、ドアロック装置２をオートロックモードに設定する設定動作を行なう（ステップＳ５１）。

【０１５９】

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロ

ック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

【０１６０】

また、ステップＳ５０で、オートロックモードではないと判別したときには、ＣＰＵ２０１は、逐次ロックモードが選択されたと判別して、ドアロック装置２を逐次ロックモードにする設定動作を行なう（ステップＳ５２）。

【０１６１】

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

【０１６２】

以上で、監視制御装置３におけるロック制御モードの設定時の動作は終了となる。

【０１６３】

次に、ドアロック装置通信インターフェース２０６を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置１００の動作について、図２０のフローチャートを参照して説明する。

【０１６４】

先ず、ドアロック制御装置１００のＣＰＵ１０１は、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったか否か判別し（ステップＳ６１）、受け取らないときには、その他の処理を行なう（ステップＳ６２）。

【０１６５】

ステップＳ６１で、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったと判別したときには、ＣＰＵ１０１は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップＳ６３）。

【０１６６】

ステップＳ６３で、選択指示されたドアロック制御モードはオートロックモー

ドであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップＳ６４）。

【０１６７】

すなわち、ステップＳ６４においては、ドアロック制御装置１００のＣＰＵ１０１は、オートロックモードの設定指示に基づき、ドアロック装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケーションを、オートロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

【０１６８】

また、ステップＳ６３で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップＳ６５）。

【０１６９】

すなわち、ステップＳ６５においては、ドアロック制御装置１００のＣＰＵ１０１は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

【０１７０】

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部ｅｘのみをアクティブにして、内側電子鍵リード／ライト部２１ｉｎを用いないようにす

ることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

【０１７１】

次に、オートロックモードと、逐次ロックモードのそれぞれの場合のドアロック装置２の動作について説明する。以下に説明するフローチャートにおける各ステップＳの動作は、ドアロック制御装置１００のＣＰＵ１０１が主として実行する処理動作である。

【０１７２】

［オートロックモード；図２１～図２６］

オートロックモードのときの動作を、図２１～図２６のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア１は、定常状態では、施錠状態とされる。そして、電子鍵装置４０が、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報、すなわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア１は施錠状態に戻るように、ドアロック制御装置１００により制御されるものである。

【０１７３】

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、電子鍵装置４０がかざされて、電子鍵装置４０と内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ７１）。

【０１７４】

そして、ステップＳ７１において、ＩＣカード４０Ｆがかざされて、リード／ライト部２１ｉｎまたは２１ｅｘと通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報をＩＣカード４０Ｆから受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ７２）。このとき、ドアロック制御装置１００

が備える時計回路（図示を省略）の時刻情報が、ＩＣカード４０Ｆに与えられ、制御用ＩＣ内４２のメモリに書き込まれる。また、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらと通信をしたかの情報として、通信相手のＩＤ等が制御用ＩＣ４２のメモリに書き込まれる。

【０１７５】

次に、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらでＩＣカード４０Ｆと通信が行われたかを判別する（ステップＳ７３）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ１２０の、前記識別情報に対応する家人の記録エリアにも書き込まれ、また、監視制御装置３にも、その家族情報メモリ２０５に記憶させるために転送される。

【０１７６】

[内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図２１～図２３]

ステップＳ７３で、ＩＣカード４０Ｆと通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

【０１７７】

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている電子鍵情報としての識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ７４）。

【０１７８】

そして、その認証結果を判別し（ステップＳ７５）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致

するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ７６）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ７１に戻る。

【０１７９】

また、ステップＳ７５で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ７７）。このとき、ＣＰＵ１０１により、併せて内側スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

【０１８０】

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ７８）、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ７９）。このとき、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させ、ドアロックの解除状態をＩＣカード４０Ｆの使用者に報知するようにしてもよい。

【０１８１】

このとき、ＣＰＵ１０１は、ＩＣカード４０Ｆにより内側から玄関ドア１が開錠されたことを認識していることに基づき、当該ＩＣカード４０Ｆの使用者（在宅者）が外出しようとしていると認識する。そして、監視制御装置３に対して窓の開閉状態についての問い合わせを送る（図２２のステップＳ８１）。

【０１８２】

これに対して、監視制御装置３では、窓センサ６ａ，６ｂのセンサ出力をセンサハブ２０７を通じて取得して、窓の開閉を確認する。つまり、戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェー

ス２０６を通じてドアロック制御装置１００に返信するようにする。

【０１８３】

ドアロック制御装置１００では、この窓の開閉状態についての確認結果を、通信インターフェース１２１を通じて受信する（ステップＳ８２）。そして、ＣＰＵ１０１は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップＳ８３）。

【０１８４】

そして、窓が開いていると判別したときには、ＣＰＵ１０１は、窓が開いていることを内側スピーカ２３ｉｎからの放音音声により警告する（ステップＳ８４）。また、窓が閉じていると判別したときには、ＣＰＵ１０１は、戸締りがＯＫであることを内側スピーカ２３ｉｎからの放音音声により報知する（ステップＳ８５）。

【０１８５】

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ８６）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ８７）、１０秒経過したと判別したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ８８）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ８９）。

【０１８６】

また、ステップＳ８６で、ステップＳ７８での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップＳ７２で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ９０）。

【０１８７】

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ９１）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ９２）、ドア

ロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（図２３のステップＳ１０１）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことをＩＣカード４０Ｆの使用者に報知する（ステップＳ１０２）。この外側ＬＥＤ２２ｅｘの緑色点滅は、所定時間、例えば１０秒間続けられる。

【０１８８】

その後、ＣＰＵ１０１は、前記所定時間、例えば１０秒経過したか否か判別し（ステップＳ１０３）、所定時間経過していないと判別したときには、ステップＳ７１で通信が行われたと判別されたＩＣカード４０Ｆが、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別する（ステップＳ１０４）、通信がなされないと判別したときにはステップＳ１０３に戻る。

【０１８９】

そして、ステップＳ１０３で、ＩＣカード４０Ｆと外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、前記所定時間経過したと判別したときには、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎに対してＩＣカード４０Ｆがかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図２１のステップＳ７１に戻る。

【０１９０】

また、ステップＳ１０４で、玄関ドア施錠復帰後、外側ＬＥＤ２２ｅｘの緑色点滅が終了する所定時間経過する前に、ステップＳ７１において通信が行われたと判別されたＩＣカード４０Ｆと外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、ステップＳ１０１～Ｓ６３で確認された戸締りを再確認する（ステップＳ１０５）。

【０１９１】

ステップＳ１０５で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１０６）。

【０１９２】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして

、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

【０１９３】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１０７）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１０８）。

【０１９４】

また、ステップＳ１０７で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１０９）。その後、ステップＳ７１に戻る。

【０１９５】

また、ステップＳ１０５で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１１０）。そして、その後、ステップＳ７１に戻る。

【０１９６】

[外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２４～図２６]

ステップＳ７１で、ＩＣカード４０Ｆと通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理

を行なう。

【０１９７】

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録されたＩＣカード４０Ｆであるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１２１）。

【０１９８】

そして、その認証結果を判別し（ステップＳ１２２）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１２３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ７１に戻る。

【０１９９】

また、ステップＳ１２２で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１２４）。このとき、ＣＰＵ１０１により、合わせて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

【０２００】

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１２５）、外側スピーカ２３ｅｘから、「ドアロックを解

除しました」というメッセージを放音させる（ステップＳ１２６）。このとき、外側ＬＥＤ２２ｅｘを、例えば緑色で点滅させ、ドアロックの解除状態をＩＣカード４０Ｆの使用者に報知するようにしてもよい。

【０２０１】

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ１２７）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ１２８）、１０秒経過したと判別したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ１２９）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１３０）。

【０２０２】

その後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（ステップＳ１３１）、所定時間経過していないと判別したときには、ステップＳ７１で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１３２）、通信がなされないと判別したときにはステップＳ１３１に戻る。

【０２０３】

そして、ステップＳ１３１で、電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、所定時間経過したと判別したときには、ＣＰＵ１０１は、外側電子鍵リード／ライト部２１ｅｘに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図２１のステップＳ７１に戻る。

【０２０４】

また、ステップＳ１３２で、玄関ドア施錠復帰後、所定時間経過する前に、ステップＳ７１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１３３）。

【０２０５】

このステップＳ１３３での戸締りの確認は、前述のステップＳ１２１～Ｓ１２３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

【０２０６】

ステップＳ１３３で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１３４）。

【０２０７】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

【０２０８】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１３５）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１３６）。

【０２０９】

また、ステップＳ１３５で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１３７）。その後、ステップ

Ｓ７１に戻る。

【０２１０】

また、ステップＳ１３３で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１３８）。そして、その後、ステップＳ７１に戻る。

【０２１１】

ステップＳ１３１～ステップＳ１３８の処理は、一旦、玄関ドア１を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部２１ｉｎに対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。

【０２１２】

すなわち、一旦、玄関ドア１を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、玄関ドア１を一旦開錠させ、その後、１０秒待って再施錠になった後、１０秒以内に、再び、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部２１ｉｎに電子鍵装置４０をかざすところからやり直す必要がなく、便利である。

【０２１３】

次に、ステップＳ１２７で、ステップＳ１２５での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップＳ７２で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置３に転送する（図２６のステップＳ１４１）。

【０２１４】

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ１４２）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ１４３）、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（ステップＳ１４４）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１４５）。

【０２１５】

その後、ＣＰＵ１０１は、帰宅者があったことから在宅状況が変更することに基づき、セキュリティレベルの変更指示を監視制御装置３に送る（ステップＳ１４６）。

【０２１６】

このセキュリティレベルの変更指示を受け取った監視制御装置３では、ステップＳ１４１での帰宅者情報による在宅状況の変化を認識し、図１５に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否か判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置３は、セキュリティレベルを変更したかどうかを、ドアロック制御装置１００に通知する。

【０２１７】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティレベルの変更に関する通知を受け取って（ステップＳ１４７）、セキュリティレベルが変更されたか否かを判別する（ステップＳ１４８）。

【０２１８】

そして、ステップＳ１４８で、セキュリティモードが変更されたと判別したときには、ＣＰＵ１０１は、内側スピーカ２３ｉｎから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップＳ１４９）。そして、ステップＳ７１に戻る。

【０２１９】

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置１００

から、ステップＳ１４６において、監視制御装置３にセキュリティレベルの変更指示を送るようにしたが、監視制御装置３では、ステップＳ１４１での帰宅者情報の転送を受けるので、ドアロック制御装置１００からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その場合には、セキュリティレベルを変更したときには、その旨をドアロック制御装置１００に転送するようにする。

【０２２０】

[逐次ロックモードの説明；図２７～図２９]

次に、逐次ロックモードのときの動作を、図２７～図２９のフローチャートを参照しながら説明する。この逐次ロックモードのときには、ＩＣカード４０Ｃが、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア１の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構２８は、ドアロック制御装置１００により制御されるものである。

【０２２１】

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、ＩＣカード４０Ｃがかざされて、ＩＣカード４０Ｃと内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ１５１）。

【０２２２】

そして、ステップＳ１５１において、ＩＣカード４０Ｆがかざされて、ＩＣカード４０Ｆと通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報をＩＣカード４０Ｆから受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ１５２）。このとき、前述と同様に、ＩＣカード４０Ｆには時刻情報等が書き込まれると共に、家族情報メモリ１２０および監視制御装置３の家族情報メモリ２０５への時刻情報等の書き込みが行なわれる。

【０２２３】

内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらでＩＣカード４０Ｆと通信が行われたかを判別する（ステップＳ１５３）。

【０２２４】

［内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図２７］

ステップＳ１５３で、ＩＣカード４０Ｆと通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出する場合あるいは玄関ドア１をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

【０２２５】

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１５４）。

【０２２６】

そして、その認証結果を判別し（ステップＳ１５５）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１５６）。そして、ドアロック機構２８は、その前の状態のままとして、ステップＳ１５１に戻る。

【０２２７】

また、ステップＳ１５５で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証

がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１５７）。このとき、ＣＰＵ１０１により、併せて内側スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

【０２２８】

そして、ＣＰＵ１０１は、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態になっているか否か判別する（ステップＳ１５８）。このステップＳ１５８で、ドアロック機構２８による玄関ドア１のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御する（ステップＳ１５９）。

【０２２９】

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをＩＣカード４０Ｆの使用者に報知するようにする（ステップＳ１６０）。

【０２３０】

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報を、在宅者情報として監視制御装置３に転送する（ステップＳ１６１）。

【０２３１】

また、ステップＳ１５８で、現在のドアロック機構２８のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８を開錠状態にし（ステップＳ１６２）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１６３）。

【０２３２】

そして、このときには、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別

情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ１６４）。

【０２３３】

[外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２８～図２９]

ステップＳ１５３で、ＩＣカード４０Ｆと通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

【０２３４】

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、ＩＣカード４０Ｆから受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあるかどうかにより、当該ＩＣカード４０Ｆがドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該ＩＣカード４０Ｆについての認証を行なう（ステップＳ１７１）。

【０２３５】

そして、その認証結果を判別し（ステップＳ１７２）、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることをＩＣカード４０Ｆの使用者に報知する（ステップＳ１７３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ１５１に戻る。

【０２３６】

また、ステップＳ１７２で、家族情報メモリ１２０に記憶されている識別情報の中に、ＩＣカード４０Ｆから受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることを

ＩＣカード４０Ｆの使用者に報知する（ステップＳ１７４）。このとき、ＣＰＵ１０１により、併せて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

【０２３７】

そして、ＣＰＵ１０１は、現在のドアロック機構２８のロック状態は、施錠状態になっているか否か判別する（ステップＳ１７５）。このステップＳ１７５で、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１７６）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１７７）。

【０２３８】

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置３に転送する（ステップＳ１７８）。

【０２３９】

また、ステップＳ１７５で、現在の玄関ドア１のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態にする（ステップＳ１７９）。

【０２４０】

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをＩＣカード４０Ｆの使用者に報知するようにする（ステップＳ１８０）。

【０２４１】

そして、ＣＰＵ１０１は、ステップＳ１５２で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報を、外

出者情報として監視制御装置３に転送する（ステップＳ１８１）。

【０２４２】

そして、施錠後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（図２９のステップＳ１８２）、所定時間経過していないと判別したときには、ステップＳ１７１で通信が行われたと判別されたＩＣカード４０Ｆが、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１８３）、通信がなされないと判別したときにはステップＳ１８２に戻る。

【０２４３】

また、ステップＳ１８３で、玄関ドア施錠後、所定時間経過する前に、ステップＳ７１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１８４）。

【０２４４】

このステップＳ１８４での戸締りの確認は、前述のステップＳ１０１～Ｓ１０３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

【０２４５】

ステップＳ１８４で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１８５）。

【０２４６】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１５に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す

。

【０２４７】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１８６）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１８７）。

【０２４８】

また、ステップＳ１８６で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１８８）。その後、ステップＳ１５１に戻る。

【０２４９】

また、ステップＳ１８４で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１８９）。そして、その後、ステップＳ１７１に戻る。

【０２５０】

[監視制御装置３におけるセキュリティ動作；図３０]

上述のようにして、監視制御装置３は、ドアロック制御装置１００からの指示を受けてセキュリティモードをオンにするが、リモートコマンダ５０のセキュリティボタン５１を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置３のセキュリティモードオン状態は、リモートコマンダ５０のオフボタン５２を操作すると、オフとすることができる。

【０２５１】

図３０は、リモートコマンダ５０を操作することにより、監視制御装置３のセキュリティモードのオン・オフを制御する動作を説明するためのフローチャート

である。

【０２５２】

まず、ＣＰＵ２０１は、リモートコマンダ５０からの遠隔操作信号を監視して、リモートコマンダ５０で操作入力がなされたか否か判別する（ステップＳ１９１）。そして、操作入力がなされたと判別したときには、ＣＰＵ２０１は、操作されたのはセキュリティボタン５１であるか否か判別する（ステップＳ１９２）。

【０２５３】

ステップＳ１９２での判別の結果、セキュリティボタン５１の操作であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ１９３）。

【０２５４】

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオンの確認画面を表示する（ステップＳ１９４）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ１９５）。

【０２５５】

そして、ＣＰＵ２０１は、その所定時間、例えば５分経過後（ステップＳ１９６）、セキュリティモードをオンにして（ステップＳ１９７）、セキュリティ監視動作を実行する（ステップＳ１９８）。ステップＳ１９６における所定時間は、セキュリティボタン５１を操作した使用者が、セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

【０２５６】

ステップＳ１９２において、リモートコマンダ５０で操作されたボタンがセキュリティボタン５１ではないと判別したときには、ＣＰＵ２０１は、操作されたのはオフボタン５２であるか否か判別する（ステップＳ１９９）。このステップ

Ｓ１９９でオフボタン５２ではないと判別したときには、ＣＰＵ２０１は、その他のボタンが押されたことによる処理を実行する（ステップＳ２００）。

【０２５７】

ステップＳ１９９での判別の結果、オフボタン５２であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ２０１）。

【０２５８】

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオフの確認画面を表示する（ステップＳ２０２）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ２０３）。

【０２５９】

そして、ＣＰＵ２０１は、セキュリティモードをオフにする処理を行なう（ステップＳ２０４）。以上で、図３０の処理ルーチンは終了となる。

【０２６０】

[セキュリティモードオンにおける監視動作]

図３１および図３２は、監視制御装置３において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンダ５０でのセキュリティボタン５１の操作時に起動されるもので、このときのセキュリティレベルは、レベルＡの場合である。なお、ドアロック制御装置１００からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

【０２６１】

図３１においては、先ず、ＣＰＵ２０１は、ビデオカメラ３１の撮影画像の取り込みを開始する（ステップＳ２１１）。このとき、マイクロホン３４で収音し

た音声も一緒に取り込みを行なう。前述したように、画像・音声メモリ２０８に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の３０秒分の画像・音声情報が常に画像・音声メモリ２０８に格納されるようにされている。監視カメラ１３からの撮影画像についても同様にされている。

【０２６２】

次に、ＣＰＵ２０１は、センサハブ２０７からの窓センサ１６ａ、１６ｂのセンサ出力と、玄関ドア１のドア開閉センサ２７のセンサ出力の監視を開始するように制御する（ステップＳ２１２）。さらに、ＣＰＵ２０１は、火災センサ４およびガスセンサ５のセンサ出力の監視を開始するように制御する（ステップＳ２１３）。監視カメラ１３は、火災センサ４やガスセンサ５のオン・オフに応じてオン・オフする。

【０２６３】

次に、ＣＰＵ２０１は、人感センサ３３のセンサ出力を監視して、侵入者がないかどうかチェックする（ステップＳ２１４）。侵入者なしと判別したときには、窓センサ１６ａ，１６ｂのセンサ出力や、ドア開閉センサ２７のセンサ出力から、異常を検知したか否か判別する（図３２のステップＳ２３１）。

【０２６４】

ステップＳ２３１で、異常を検知しないと判別したときには、ＣＰＵ２０１は、火災センサ４やガスセンサ５のセンサ出力から、異常を検知したか否か判別する（ステップＳ２３２）。ステップＳ２３２で、異常を検知しないと判別したときには、ステップＳ２１４に戻る。

【０２６５】

そして、ステップＳ２１４で、侵入者を人感センサ３３により検知したと判別したときには、ＣＰＵ２０１は、照明機構３２０を制御して、照明３２をオンにする（ステップＳ２１５）。そして、侵入者の検知時点の１０秒前から、検知時点の２０秒後までの３０秒分の画像・音声情報を、画像・音声メモリ２０８から読み出し、１回目の画像として、管理サーバ装置１０に転送する（ステップＳ２１６）。管理サーバ装置１０では、この転送されてきた画像・音声情報により、

侵入者を認識して、適切な処置を取ることができる。

【０２６６】

次に、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ２１７）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ２１８）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【０２６７】

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２１９）。

【０２６８】

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２２０）。そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったか否か判別し（ステップＳ２２１）、検知しなくなるまで、３０秒分の画像・音声情報を管理サーバ装置１０に転送する処理作業を継続する。

【０２６９】

そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったと判別したときには、３０秒分の画像・音声情報の管理サーバ装置１０への転送を中止する（ステップＳ２２２）。そして、ステップＳ２３１に戻って、セキュリティ監視を続ける。

【０２７０】

また、ステップＳ２３１において、異常を検知したと判別したときには、ＣＰＵ２０１は、窓センサ６ａ，６ｂやドア開閉センサ２７の近傍に設置されている監視カメラ１３からの検知時点の１０秒前から、検知時点の２０秒後までの３０秒分画像を１回目として、管理サーバ装置１０に転送する（ステップＳ２３４）

。

【０２７１】

そして、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ２３５）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ２３６）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【０２７２】

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２３７）。

【０２７３】

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２３８）。そして、ＣＰＵ２０１は、リモートコマンダ５０のオフボタン５２によるオフ指示を待ち（ステップＳ２３９）、オフ指示が有ったときには、セキュリティモードをオフとする。

【０２７４】

また、ステップＳ２３２で、火災センサ４またはガスセンサ５で異常が検知されたと判別したときには、ＣＰＵ２０１は、監視制御装置３に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２３３）。そして、ステップＳ２３９に進む。

【０２７５】

なお、画像・音声情報を監視制御装置３から受け取った管理サーバ装置１０は、Ｗｅｂページにそれらの画像・音声情報を載せる。そこで、監視制御装置３から連絡を受け取った携帯電話の持ち主は、管理サーバ装置１０の当該Ｗｅｂページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

【０２７６】

［監視制御装置３におけるドアロック制御装置１００からの指示による連携；図３３］

監視制御装置３のＣＰＵ２０１は、ドアロック制御装置１００から受け取った情報や指示に応じて、図３３に示すような連携動作を行なう。なお、この例は、セキュリティレベルの変更は、ＣＰＵ２０１が、ドアロック制御装置１００からの変更指示を受けて行なうのではなく、ドアロック制御装置１００からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なうようにした場合である。

【０２７７】

すなわち、ＣＰＵ２０１は、ドアロック制御装置１００からセキュリティモードオンの指示を受け取ったか否か判別する（ステップＳ２４１）。受け取らないと判別したときには、ＣＰＵ２０１は、その他の処理を行なう（ステップＳ２４２）。

【０２７８】

ステップＳ２４１でセキュリティモードオンの指示を受信したと判別したときには、ＣＰＵ２０１は、家族情報メモリ２０５の記憶情報を参照して、在宅状況をチェックする（ステップＳ２４３）。そして、図１５に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する（ステップＳ２４４）。

【０２７９】

ステップＳ２４４で、セキュリティモードオンにすることができないと判別したときには、ＣＰＵ２０１は、その旨をドアロック制御装置１００に通知する（ステップＳ２４５）。

【０２８０】

一方、ステップＳ２４４で、セキュリティモードオンにすることが可能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置１００に通知し（ステップＳ２４６）、所定時間経過するのを待つ（ステップＳ２４７）。

【０２８１】

所定時間経過したことを確認したら、ＣＰＵ２０１は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップＳ２４８）。そして、セキュリティ監視動作を開始する（ステップＳ２４９）。

【０２８２】

このセキュリティ監視動作中において、ドアロック制御装置１００から識別情報を含む個人情報を受信したか否か判別し（ステップＳ２５０）、受信しなければステップＳ２４９に戻って、セキュリティ監視動作を継続する。ドアロック制御装置１００から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップＳ２５１）、セキュリティレベルの変更が必要であるか判別する（ステップＳ２５２）。

【０２８３】

セキュリティレベルの変更が必要ではないと判別したときには、ＣＰＵ２０１は、ステップＳ２４９に戻って、セキュリティ監視動作を継続する。また、ステップＳ２５２で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップＳ２５３）、そうではないときには、在宅状況に応じてセキュリティレベルを変更する（ステップＳ２５４）。そして、セキュリティレベルを変更した旨をドアロック制御装置１００に通知する（ステップＳ２５５）。

【０２８４】

また、ステップＳ２５３で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップＳ２５６）、その旨をドアロック制御装置１００に通知する（ステップＳ２５７）。そして、ステップＳ２４１に戻る。

【０２８５】

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

【０２８６】

また、電子鍵装置の所有者の生体情報により、電子鍵装置において、当該電子鍵装置の使用者が所有者であるか否かについてのチェック（認証）を行ない、認証がＯＫであるときにのみ、電子鍵情報を送出するようにするので、電子鍵装置を紛失したとしても、所有者以外が電子鍵装置を使用して、ドアロック制御をすることは不可能であるので、セキュリティ上の安全性が非常に高い。

【０２８７】

また、ドアロック装置２を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝ってに合わせて、いずれのモードにするかを選択することができて、非常に便利である。

【０２８８】

また、内側電子鍵リード／ライト部２１ｉｎを設けて、この内側電子鍵リード／ライト部２１ｉｎによっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

【０２８９】

また、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとを設けることにより、これらと電子鍵装置との通信により、家族の入退出の管理をすることが容易である。

【０２９０】

そのため、ドアロック装置２と、監視制御装置３とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければならないなどのあわただしさを解消することができる。

【０２９１】

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるので、窓の閉め忘れを防止することができる。

【０２９２】

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変する

ことができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロックの開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

【０２９３】

[電子鍵装置の電子鍵情報の登録]

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置２の販売業者あるいは設置業者もしくは使用者により行なわれる。

【０２９４】

先ず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装置は、ＩＣカードとしており、ドアロック装置２の販売業者あるいは設置業者から、ドアロック装置２の各戸への設置に際して、使用者に渡される。

【０２９５】

この実施形態の場合、ドアロック装置２の各戸への設置前に、当該ドアロック装置２を設置する戸の家族構成員の各人についての個人情報が収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶するＩＣカードが割り当てられ、それぞれのＩＣカードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロファイル情報が構成される。

【０２９６】

そして、設置されるドアロック装置２のシリアル番号等からなる製品番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロファイル情報が、予め管理サーバ装置１０のドアロック装置管理データベース３０５に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロファイル情報に含められて予め管理サーバ装置１０に登録されている。

【０２９７】

この際に、ドアロック装置管理データベースにおいては、家族構成員の個人プロファイル情報は、監視制御装置３の通信ネットワーク上のアドレス情報に対応して記憶される。当該アドレス情報としては、前述したように、この例では、電話番号やＩＰアドレスが用いられる。

【０２９８】

管理サーバ装置１０に登録された本鍵情報および各家族構成員の個人プロファイル情報は、ドアロック装置２の設置業者や販売業者が、ドアロック装置２の設置を完了したときに、管理会社の管理サーバ装置１０に初期登録要求をしたときに、管理サーバ装置１０から監視制御装置３に転送されることにより、監視制御装置３の家族情報メモリ２０５に書き込まれて登録される。また、監視制御装置３に登録された情報のうち、少なくとも本鍵情報は、ドアロック制御装置１００に転送されることにより、その家族情報メモリ１２０登録される。

【０２９９】

図３４は、初期登録要求を受けたときの管理サーバ装置１０の動作を示すものである。図３４の各ステップの動作は、主としてＣＰＵ３０１が主体となって行なうものである。

【０３００】

先ず、ＣＰＵ３０１は、初期登録要求を受け付けたか否か判別する（ステップＳ２６１）。この初期登録要求は、ドアロック装置２のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置１０に送られる場合と、電話等で、初期登録要求を受けたオペレータが図示しない入力手段により入力する場合とがある。

【０３０１】

ＣＰＵ３０１は、この初期登録要求を受け取ると、装置識別情報を検索子として、ドアロック装置データベースを検索し、予め登録されているドアロック装置２および監視制御装置３の通信ネットワーク９上でのアドレス情報を読み出して、初期登録要求を含む発呼をする。つまり、初期登録要求されたドアロック装置

２が接続されている監視制御装置３に対して初期登録要求の発呼を行なう（ステップＳ２６２）。

【０３０２】

このとき、監視制御装置３は、自動応答を行なうので、ＣＰＵ３０１は、当該監視制御装置３からの応答を確認して、当該監視制御装置３との間に通信路を形成する（ステップＳ２６３）。

【０３０３】

次に、ＣＰＵ３０１は、ドアロック装置２に関連して上述のように管理サーバ装置１０のドアロック装置データベース２０５に記憶している、ドアロック装置が設置された家の家族構成員全員についての本鍵情報を含む個人プロファイル情報を監視制御装置３に送信する（ステップＳ２６４）。

【０３０４】

次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から登録完了通知が到来するのを待ち（ステップＳ２６５）、登録完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ２６６）、この初期登録の処理ルーチンを終了する。

【０３０５】

この初期登録要求情報を受け取る監視制御装置３の動作を、図３５のフローチャートを参照して説明する。

【０３０６】

監視制御装置３のＣＰＵ２０１は、管理サーバ装置１０からの着信を受信したか否か判別し（ステップＳ２７１）、管理サーバ装置１０からの着信の受信でなかったと判別したときには、その他の処理を行なう（ステップＳ２７２）。

【０３０７】

管理サーバ装置１０からの着信を受信したと判別したときには、ＣＰＵ２０１は、その着信に自動応答して管理サーバ装置１０との間に通信路を形成する（ステップＳ２７３）。そして、受信した着信は初期登録要求であるか否か判別する（ステップＳ２７４）。初期登録要求であると判別すると、ＣＰＵ２０１は、管理サーバ装置１０からの登録情報を待ち、登録情報を受信したら（ステップＳ２

７５）、受信した登録情報を、家族情報メモリ２０５に書き込む（ステップＳ２７６）。

【０３０８】

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置１０に登録完了通知を返送し（ステップＳ２７７）、管理サーバ装置１０との通信路を切断する（ステップＳ２７８）。

【０３０９】

次に、ＣＰＵ２０１は、家族情報メモリ２０５に書き込んで登録した個人プロファイル情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置１００に転送する（ステップＳ２７９）。ドアロック制御装置１００は、この情報を受けて、家族情報メモリ１２０に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置１００に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０３１０】

そして、ＣＰＵ２０１は、ドアロック制御装置１００への本鍵情報および必要は情報の転送の終了を確認すると（ステップＳ２８０）、この処理ルーチンを終了する。

【０３１１】

なお、ステップＳ２７４で、初期登録ではないと判別したときには、ＣＰＵ２０１は、後述するバックアップ鍵の登録要求であるか否か判別し（ステップＳ２８１）、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する（ステップＳ２８２）。このバックアップ登録の処理については後述する。

【０３１２】

また、ステップＳ２８１でバックアップ登録要求ではないと判別したときには、ＣＰＵ２０１は、紛失鍵の抹消要求であるか否か判別する（ステップＳ２８３）。そして、紛失鍵の抹消要求でないと判別したときには、ＣＰＵ２０１は、そ

の他の処理を実行し（ステップＳ２８４）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップＳ２８５）。以上で、図３５の処理を終了する。

【０３１３】

[バックアップ鍵登録について]

この実施形態においては、管理サーバ装置１０が備える鍵登録ホームページにアクセスすることにより、バックアップ鍵の登録を行なうことができる。図３６は、このバックアップ鍵登録の際のシステム構成を説明するための図である。また、図３７および図３８は、このときの管理サーバ装置１０の動作を説明するためのフローチャートである。

【０３１４】

図３６に示すように、先ず、電子鍵リード／ライト装置２００１を備える、あるいは電子鍵リード／ライト装置２００１が接続されているパーソナルコンピュータ２００２を用意する。そして、電子鍵リード／ライト装置２００１にバックアップ鍵として登録したい電子鍵装置４０Ｂ、例えばＩＣカード、携帯電話端末、ＰＤＡをセットする。

【０３１５】

これらの電子鍵装置４０Ｂは、前述したＩＣカード４０Ｆや４０Ｉと同様に、所有者の指紋や虹彩などの生体情報が登録されたメモリ、生体情報の取得部、電磁誘導アンテナなどからなる通信手段、電子鍵装置ごとに異なるように一元管理された識別情報からなる電子鍵情報が格納されたメモリを備えるＩＣチップを備える。そして、各電子鍵装置４０ＢのＩＣチップは、前述と同様に、生体情報取得部からの生体情報についての認証を行なって、認証が取れたときに電磁誘導アンテナなどの通信手段を介して電子鍵情報を送出するようにするものである。

【０３１６】

次に、パーソナルコンピュータ２００２からインターネット２００３を通じて管理サーバ装置１０の鍵登録ホームページにアクセスする。

【０３１７】

管理サーバ装置１０では、この鍵登録ホームページへのアクセスの有無を監視

しており（ステップＳ３０１）、アクセスがないときには、その他の処理を行なっている（ステップＳ３０２）。そして、鍵登録ホームページへのアクセスを受信したときには、ＣＰＵ３０１は、鍵登録ホームページの表示情報を送信する（ステップＳ３０３）。

【０３１８】

この鍵登録ホームページは、パーソナルコンピュータ２００２の画面に表示される。この画面には、登録者の認証確認用情報の入力を促すメッセージと、入力欄が表示されているので、予め定められたパスワードや顧客ＩＤ、ドアロック装置２が設置された住所、電話番号、鍵登録を要求している者の氏名などの必要な認証確認用情報を入力した後、当該認証確認用情報を管理サーバ装置１０に送る。

【０３１９】

管理サーバ装置１０では、この認証確認用情報を受信したか否か判別し（ステップＳ３０４）、受信したら認証がＯＫであるか否か判別する（ステップＳ３０５）。認証が取れなかったとき（認証ＮＧのとき）には、認証ＮＧを報知する画面をパーソナルコンピュータ２００２に送る（ステップＳ３０６）。

【０３２０】

この認証ＮＧを報知する画面では、認証確認用情報の再入力をすることができると共に、アクセスを中断することもできる。鍵登録者は、いずれかの操作をすることになる。

【０３２１】

そこで、管理サーバ装置１０のＣＰＵ３０１は、認証確認用の情報を再受信したか否か判別し（ステップＳ３０７）、再受信しなかったときには、アクセスが中断されたかどうか判別し（ステップＳ３０８）、アクセス中断と判別されなかったときには、ステップＳ３０７に戻る。そして、ステップＳ３０７で、認証確認用の情報を再受信したと判別したときには、ＣＰＵ３０１は、ステップＳ３０５に戻って、認証が取れるかどうか判別する。ステップＳ３０８で中断であると判別したときには、アクセス切断処理を行なう（ステップＳ３０９）。

【０３２２】

ステップＳ３０５において、認証がＯＫであると判別したときには、ＣＰＵ３０１は、バックアップ鍵登録用画面を送信する（図３６のステップＳ３１１）。このバックアップ鍵登録用画面には、鍵登録ボタンと、アクセス中断ボタンがある。鍵登録者は、いずれかのボタンを操作することになる。鍵登録を行なうときには、鍵登録者は、指紋や虹彩などの生体情報の入力を電子鍵装置４０Ｂに対して行なうと共に、鍵登録ボタンを押す。

【０３２３】

そして、鍵登録ボタンが押されたときには、パーソナルコンピュータ２００２は、バックアップ登録したい電子鍵装置４０Ｂから電子鍵リード／ライト部２００１により識別情報を読み取って、バックアップ鍵情報として管理サーバ装置１０に送る。

【０３２４】

そこで、管理サーバ装置１０のＣＰＵ３０１は、バックアップ鍵情報を受信したか否か判別し（ステップＳ３１２）、受信しなかったときには、アクセスが中断されたかどうか判別し（ステップＳ３１３）、アクセス中断と判別されなかったときには、ステップＳ３１２に戻る。

【０３２５】

そして、ステップＳ３１３で中断であると判別したときには、アクセス切断処理を行なって（ステップＳ３０９）、鍵ホームページを閉じる。また、ステップＳ３１２で、バックアップ鍵情報を受信したと判別したときには、ＣＰＵ３０１は、ドアロック装置データベース３０５に、鍵登録要求者のバックアップ鍵情報として、受信した電子鍵情報を登録する（ステップＳ３１５）。このとき、電子鍵登録・紛失履歴メモリ３０６にも、その登録したバックアップ鍵情報と、鍵登録要求者の識別情報とがバックアップ登録履歴として、カレンダー情報および時刻情報と共に書き込まれる。

【０３２６】

そして、アクセス切断を行なった後（ステップＳ３１６）、鍵登録要求者が登録されているドアロック装置２が接続されている監視制御装置３に、バックアップ鍵登録要求の発信を行なう（ステップＳ３１７）。監視制御装置３では、この

バックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、ＣＰＵ３０１は、当該監視制御装置３との間に通信路を形成する（ステップＳ３１８）。

【０３２７】

次に、ＣＰＵ３０１は、鍵登録要求者を識別する情報と、バックアップ鍵情報とを監視制御装置３に送信する（ステップＳ３１９）。次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から登録完了通知が到来するのを待ち（ステップＳ３２０）、登録完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ３２１）、このバックアップ鍵登録の処理ルーチンを終了する。

【０３２８】

次に、前記ステップＳ３１７～ステップＳ３１９での送信動作により管理サーバ装置１０から送られてくるバックアップ鍵情報を受け取る監視制御装置３の動作を、図３９のフローチャートを参照して説明する。この処理ルーチンは、図３５におけるステップＳ２８２の処理に相当する。

【０３２９】

監視制御装置３のＣＰＵ２０１は、まず、バックアップ鍵情報と、鍵登録要求者の名前などの識別情報とを受信し（ステップＳ３３１）、鍵登録要求者を認識する（ステップＳ３３２）。次に、受信したバックアップ鍵情報を、認識した登録要求者のバックアップ鍵情報として、家族情報メモリ２０５に書き込んで登録する（ステップＳ３３３）。

【０３３０】

このとき、当該鍵登録要求者の個人プロファイル情報の電子鍵登録・紛失履歴エリアに、その登録したバックアップ鍵情報とカレンダー情報および時刻情報とがバックアップ登録履歴として書き込まれる。

【０３３１】

そして、ＣＰＵ２０１は、管理サーバ装置１０に、バックアップ鍵情報の登録完了通知を送る（ステップＳ３３４）。そして、管理サーバ装置１０との通信路を切断する（ステップＳ３３５）。

【０３３２】

次に、ＣＰＵ２０１は、家族情報メモリ２０５に書き込んで登録したバックアップ鍵情報である識別情報を、鍵登録要求者の識別情報と共に、ドアロック制御装置１００に転送する（ステップＳ３３６）。ドアロック制御装置１００は、この情報を受けて、家族情報メモリ１２０に、受信したバックアップ鍵情報を登録する。そして、ＣＰＵ２０１は、ドアロック制御装置１００への本鍵情報および必要は情報の転送の終了を確認すると（ステップＳ３３７）、この処理ルーチンを終了する。

【０３３３】

なお、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、ステップＳ３３６およびステップＳ３３７の処理は、行なわなくてもよい。つまり、ドアロック制御装置１００には、常に本鍵情報が存在すればよいからである。その場合には、後述する紛失鍵抹消登録の際に、紛失鍵情報の抹消と共に、新たに本鍵情報として使用する、予め監視制御装置３にバックアップ登録されていた鍵情報が、監視制御装置３からドアロック制御装置１００に転送されるようにされる。

【０３３４】

なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０３３５】

なお、以上の電子鍵情報としての識別情報の登録動作は一例であって、例えばパーソナルコンピュータ２００２および電子鍵リード／ライト装置２００１の代わりに、監視制御装置３を用いて、同様にして管理サーバ装置１０にアクセスして、バックアップ鍵を登録するようにしても良い。

【０３３６】

また、管理サーバ装置１０を介することなく、監視制御装置３およびドアロック制御装置１００に、電子鍵情報としての識別情報を登録することができるようにしても良い。

【０３３７】

なお、バックアップ鍵登録の際の鍵登録者の認証のために、本鍵情報を管理サーバ装置に送り、その後、バックアップ鍵登録したい電子鍵装置をセットして登録を行なうようにしてもよい。その場合には、鍵登録者の認証は、本鍵情報により行なうことができるので、上述の例における鍵登録者の認証確認用情報の入力は不要となる。

【０３３８】

この例の鍵登録方法によれば、電子鍵装置４０Ｂの所有者本人以外の者が登録することができないので、セキュリティ上、非常に好ましい。

【０３３９】

[鍵の紛失対策]

電子鍵装置を紛失してしまった場合には、当該紛失した電子鍵装置の悪意の取得者の利用を防止するため、この実施形態では、電子鍵情報の抹消処理を行なうようにする。図４０は、本鍵情報の抹消処理を行なう場合のシステム構成を示す図である。また、図４１は、そのときの処理手順を説明するためのフローチャートである。

【０３４０】

まず、紛失者は、管理会社に対して紛失届を提出する（手順Ｓ３４１）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順Ｓ３４２）、本人確認がＯＫであったときに、紛失届が受理される（手順Ｓ３４３）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【０３４１】

次に、管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵の抹消登録の指示入力を行なう。これを受けて、管理サーバ装置１０では、紛失鍵の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう（手順Ｓ３４４）。管理サーバ装置１０のＣＰＵ３０１は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ３０６に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む

。

【０３４２】

また、管理サーバ装置１０のＣＰＵ３０１は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理、抹消履歴の書き込みを完了すると、鍵紛失届を出した者が登録されているドアロック装置２が接続されている監視制御装置３を、データベース３０５から検索して、自動的に、当該監視制御装置３にアクセスして、紛失鍵の抹消要求を送る（手順Ｓ３４５）。

【０３４３】

紛失鍵の抹消要求を受信した監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロファイル情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置２に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順Ｓ３４６）。

【０３４４】

ドアロック装置２は、監視制御装置３からの指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行する（手順Ｓ３４７）。

【０３４５】

なお、前述もしたように、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置１００には登録されない。その場合には、手順Ｓ３４６では、紛失鍵の抹消指示と共に、監視制御装置３にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置１００に送る。

【０３４６】

そして、その場合、ドアロック制御装置１００では、手順Ｓ３４７において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【０３４７】

図４２を参照して、手順Ｓ３４４および手順Ｓ３４５における管理サーバ装置１０の動作を説明する。

【０３４８】

管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置１０のＣＰＵ３０１は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップＳ３５１）。ＣＰＵ３０１は、抹消要求がなければ、その他の処理を行なう（ステップＳ３５２）。

【０３４９】

ステップＳ３５１で、紛失鍵の抹消要求が入力されたと判別したときには、ＣＰＵ３０１は、ドアロック装置データベース３０５において抹消要求者および紛失鍵の情報を検索し（ステップＳ３５３）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ３０６に紛失者および紛失鍵の情報を書き込む（ステップＳ３５４）。

【０３５０】

次に、ＣＰＵ３０１は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップＳ３５５）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップＳ３５６）。

【０３５１】

そして、抹消要求者が登録されている監視制御装置３の通信ネットワーク９上のアドレスを、データベース３０５から検索して（ステップＳ３５７）、当該監視制御装置３に紛失鍵の抹消要求の発信を行なう（ステップＳ３５８）。ステップＳ３５５で、バックアップ鍵情報が登録されていないと判別したときには、ステップＳ３５７に即座に進む。

【０３５２】

監視制御装置３では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、ＣＰＵ３０１は、当該監視制御装置３との間に通信路を形成する（ステップＳ３５９）。

【０３５３】

次に、ＣＰＵ３０１は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置３に送信する（ステップＳ３６０）。次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から抹消完了通知が到来するのを待ち（ステップＳ３６１）、抹消完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ３６２）、この紛失鍵情報の抹消処理ルーチンを終了する。

【０３５４】

次に、前記手順Ｓ３４６において、管理サーバ装置１０から送られてくる紛失鍵の抹消要求を受け取ったときの監視制御装置３の動作を、図４３のフローチャートを参照して説明する。この処理ルーチンは、図３５におけるステップＳ２８５の処理に相当する。

【０３５５】

監視制御装置３のＣＰＵ２０１は、まず、紛失鍵情報と、抹消要求者の名前などの識別情報とを受信し（ステップＳ３７１）、抹消要求者および紛失鍵情報を認識する（ステップＳ３７２）。次に、認識した抹消要求者の紛失鍵情報を、家族情報メモリ２０５から抹消する（ステップＳ３７３）。そして、抹消要求者の個人プロファイル情報中の電子鍵登録・抹消履歴情報として、抹消した電子鍵情報としての識別情報および日付、時刻等を、家族情報メモリ２０５に書き込んだ後、管理サーバ装置１０に、抹消完了通知を送る（ステップＳ３７４）。そして、管理サーバ装置１０との通信路を切断する（ステップＳ３７５）。

【０３５６】

次に、ＣＰＵ２０１は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップＳ３７６）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップＳ３７７）。そして、ドアロック制御装置１００に紛失鍵の抹消指示を送る（ステップＳ３７８）。ステップＳ３７６で、バックアップ鍵情報が登録されていないと判別したときには、ステップＳ３７８に即座に進む。

【０３５７】

ドアロック制御装置１００では、抹消指示に従って、紛失鍵情報の抹消を実行した後、抹消完了通知を監視制御装置３に送る。そこで、監視制御装置３は、抹消完了通知の受信を待って（ステップＳ３７９）、この処理ルーチンを終了する。

【０３５８】

なお、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵情報が存在するときには、ステップＳ３７８では、紛失鍵の情報と共に、本鍵情報に格上げするバックアップ鍵情報を送るようにする。本鍵情報に格上げするバックアップ鍵情報は、抹消完了の後に、監視制御装置３から、ドアロック制御装置１００に送るようにしてもよい。

【０３５９】

なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０３６０】

図４１～図４３の例では、管理サーバ装置１０では、紛失鍵の登録抹消は、まず、管理サーバ装置１０で行なった後、監視制御装置３およびドアロック制御装置１００で行なわすようにしたが、通信ネットワーク９における支障などによって、監視制御装置３およびドアロック制御装置２における紛失鍵の抹消処理が遅れることがある。

【０３６１】

しかし、紛失鍵の登録抹消は、セキュリティ管理上では、監視制御装置３およびドアロック制御装置２での登録抹消が早い方がよい。また、管理サーバ装置１０の登録内容と、監視制御装置３およびドアロック制御装置２での登録内容とは、できるだけ同一にしておくほうが管理上、好ましい。

【０３６２】

次に説明する紛失鍵の登録抹消処理手順は、以上の点を考慮したものである。

【０３６３】

図４４は、その場合における本鍵情報の抹消処理を行なう場合の処理手順を説明するためのフローチャートである。

【０３６４】

まず、紛失者は、管理会社に対して紛失届を提出する（手順Ｓ３８１）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順Ｓ３８２）、本人確認がＯＫであったときに、紛失届が受理される（手順Ｓ３８３）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【０３６５】

次に、管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵の抹消登録の指示入力を行なう。これを受けて、管理サーバ装置１０は、紛失鍵情報が登録されている監視制御装置３およびドアロック制御装置２のアドレスを、データベース３０５から検索して、検索結果の監視制御装置に対して、紛失鍵の抹消要求を送る（手順３８４）。

【０３６６】

紛失鍵の抹消要求を受信した監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロファイル情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置２に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順Ｓ３８５）。

【０３６７】

ドアロック装置２は、監視制御装置３からの指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行し、抹消完了通知を監視制御装置３に返送する（手順Ｓ３８６）。

【０３６８】

このドアロック装置２からの抹消完了通知を受けた監視制御装置３は、抹消完了通知を管理サーバ装置１０に返送する（手順Ｓ３８７）。

【０３６９】

抹消完了通知を受けた管理サーバ装置１０は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、管理サーバ装置１０のＣＰＵ３０１は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ３０６に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む（手順Ｓ３８８）。

【０３７０】

なお、前述もしたように、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置１００には登録されない。その場合には、手順Ｓ３８５では、紛失鍵の抹消指示と共に、監視制御装置３にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置１００に送る。

【０３７１】

そして、その場合、ドアロック制御装置１００では、手順Ｓ３８６において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【０３７２】

図４５を参照して、この例の場合における管理サーバ装置１０の動作を説明する。

【０３７３】

管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置１０のＣＰＵ３０１は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップＳ３９１）。ＣＰＵ３０１は、抹消要求がなければ、その他の処理を行なう（ステップＳ３９２）。

【０３７４】

ステップＳ３９１で、紛失鍵の抹消要求が入力されたと判別したときには、ＣＰＵ３０１は、ドアロック装置データベース３０５において抹消要求者および紛

失鍵の情報および監視制御装置３およびドアロック装置２のアドレスを検索し（ステップＳ３９３）、検索した監視制御装置３に対して通信ネットワーク９を通じて、紛失鍵の抹消要求を送る（ステップＳ３９４）。

【０３７５】

監視制御装置３では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、ＣＰＵ３０１は、当該監視制御装置３との間に通信路を形成する（ステップＳ３９５）。

【０３７６】

次に、ＣＰＵ３０１は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置３に送信する（ステップＳ３９６）。次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から抹消完了通知が到来するのを待つ（ステップＳ３９７）。

【０３７７】

そして、ステップＳ３９７で、抹消完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断し（ステップＳ３９８）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ３０６に紛失者および紛失鍵の情報を書き込む（ステップＳ３９９）。

【０３７８】

次に、ＣＰＵ３０１は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップＳ４００）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップＳ４０１）。そして、この紛失鍵情報の抹消処理ルーチンを終了する。

【０３７９】

[他の実施形態]

上述の実施形態は、セキュリティ監視システムも含む通信システムの構成であったので、管理サーバ装置１０が存在しているが、セキュリティ監視システムが存在しない通信システムの構成も可能である。

【０３８０】

その場合には、監視制御装置３で行なえる機能に、バックアップ鍵登録や紛失鍵抹消を用意する。そして、リモートコマンダ５０により、メニューからそれらの機能を選択して、バックアップ鍵登録や、紛失鍵の抹消を行なうようにする。

【０３８１】

例えば、バックアップ鍵情報の登録は、リモートコマンダ５０により、メニューからバックアップ鍵登録を選択し、監視制御装置３に対して、バックアップ鍵情報を登録したい電子鍵装置をかざし、リモートコマンダ５０により、登録要求者の入力を行ない、登録実行を選択することにより、行なうことができる。

【０３８２】

鍵情報の抹消も同様にして、監視制御装置３において行なうことができる。この例の場合にも、監視制御装置３からドアロック制御装置１００に鍵情報を転送したり、抹消指示をしたりするのは、上述の場合と同様である。

【０３８３】

また、ドアの施錠および開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置３は不要である。その場合には、ドアロック制御装置１００に対して、バックアップ鍵情報の登録を行なったり、紛失鍵情報の抹消を行なったりすることができる構成とすればよい。

【０３８４】

なお、電子鍵情報は、管理サーバ装置からドアロック装置の電子鍵情報の記憶部に転送して、登録するのではなく、住戸に設置する前に、予め、ドアロック装置に登録して記憶しておくようにしても勿論よい。特に、上述の実施形態のようなセキュリティ監視システムを用いずに、ドアロック制御システムを単独で使用するような場合には、そのようにするものである。

【０３８５】

上述の例では、バックアップ鍵情報が登録されていても、本鍵情報のみを電子鍵装置からの識別情報の受信時の認証用としたが、家族情報メモリ１２０または２０５に登録されているバックアップ鍵情報をも含む全てを認証用として、常時、用いるようにしても勿論よい。

【０３８６】

その場合には、鍵紛失による抹消は、当該鍵情報の抹消を行なうだけでよく、上述の例のように、バックアップ鍵を本鍵情報に格上げするようにする処理は不要となる。

【０３８７】

なお、上述の実施形態では、本鍵情報は、予め管理サーバ装置にドアロック装置の設置会社や販売会社などにより、登録しておくようにしたが、本鍵情報もバックアップ情報と同様にして、上述のようにして後から登録することができるようにしてもよい。

【０３８８】

また、上述の実施形態では、パーソナルコンピュータを用いてバックアップ鍵の登録を行なうようにしたが、監視制御装置３から管理サーバ装置１０にアクセスすることにより、行なうこともできる。その場合には、監視制御装置３が備える電子鍵リード／ライト部３６を利用することができるので、電子鍵リード／ライト装置を別個に用意する必要はない。

【０３８９】

また、パーソナルコンピュータの代わりに、電子鍵リード／ライト装置に接続される携帯電話端末から、管理サーバ装置のホームページにアクセスして、バックアップ鍵登録を行なうようにすることもできる。

【０３９０】

また、上述の実施形態では、電子鍵情報の紛失届による抹消は、本鍵情報について説明したが、紛失届の際に、本鍵情報の紛失届か、バックアップ鍵情報の紛失届かの指定をすることにより、バックアップ鍵情報の紛失届およびそれに基づくバックアップ鍵情報の抹消処理をすることもできる。

【０３９１】

また、ＩＣチップのメモリには、予め一元管理された識別情報が記憶されているように説明したが、後から、一元管理されている識別情報が書き込まれるようにされてもよいことは言うまでもない。

【０３９２】

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライト部２１

ｅｘに対して、ドアの施錠後、所定時間以内にかざした場合に、セキュリティモードをオンにするようにしたが、ドアロック制御装置１００または監視制御装置３では、玄関ドア１からの入退出を管理しているので、在宅者が無くなったら、自動的にセキュリティレベルＡでセキュリティモードをオンにするようにすることもできる。

【０３９３】

その場合に、ドアロック制御装置１００で、在宅者無しを検出したときに、監視制御装置３にセキュリティモードオンを要求しても良いし、監視制御装置３が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

【０３９４】

なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティモードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置３が、帰宅者があった場合と全く同様にして、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

【０３９５】

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、ドアロック装置で行なうようにしたが、ドアロック装置２は、監視制御装置３に、あるいは監視制御装置３を介して管理サーバ装置１０に鍵情報を送り、監視制御装置３あるいは管理サーバ装置１０で、認証作業を行ない、その認証結果を、ドアロック装置２に返す（管理サーバ装置１０の場合には監視制御装置３を介して返す）ようにしても良い。その場合には、監視制御装置３からドアロック制御装置１００への鍵情報の転送や抹消指示を送る必要はない。

【０３９６】

また、開錠者、施錠者の識別情報も監視制御装置３ではなく、管理サーバ装置１０に送り、管理サーバ装置１０により、セキュリティ管理をするようにしても

よい。

【０３９７】

また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置１００で判別するようにしたが、監視制御装置３においても、ドアロック制御装置１００でのドアロック制御モードの設定情報を備えているので、ドアロック制御装置１００は、ＩＣカード４０Ｆが、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報についての認証がとれたときには、その識別情報と、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのいずれと通信したかの情報と、開錠か施錠かの情報とを、監視制御装置３に送り、監視制御装置３が、外出か帰宅かを判別するようにすることもできる。

【０３９８】

なお、一つのドアロック装置に一つの電子鍵情報として、当該家に住む家族構成員の全員に共通の一つの電子鍵情報を用いるようにして、各人が、その共通鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできる。

【０３９９】

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情報の通信を行なうものであっても勿論よい。

【０４００】

【発明の効果】

以上説明したように、この発明によれば、予め登録された所有者の生体情報が確認されたときにのみ、電子鍵情報を送出するように制御することができるので、当該電子鍵装置を紛失したとしても、電子鍵装置の電子鍵情報記憶部に登録された生体情報と一致しない悪意の拾得者の使用を阻止することができるものである。

【０４０１】

そして、電子鍵情報として、同一のものが存在しないように一元管理されて割り振られた識別情報を用いた場合には、個人の生体情報が確認されたときにのみ

、電子鍵情報を送出するように制御することができるので、電子鍵情報は、個人識別情報として使用することができる。

【図面の簡単な説明】

【図１】

この発明のドアロック制御システムの実施の形態で用いる識別情報の概要を説明するための図である。

【図２】

この発明の実施形態で用いる識別情報の一例を示す図である。

【図３】

この発明によるドアロック制御システムの実施形態が適用された通信システムの概要を説明するための図である。

【図４】

この発明による電子鍵装置の一実施形態を示す図である。

【図５】

この発明による電子鍵装置の一実施形態の構成例を示すブロック図である。

【図６】

この発明による電子鍵装置の一実施形態の動作を説明するためのフローチャートである。

【図７】

この発明による電子鍵装置の他の実施形態を示す図である。

【図８】

この発明による電子鍵装置の他の実施形態の構成例を示すブロック図である。

【図９】

この発明による電子鍵装置の他の実施形態の動作を説明するためのフローチャートである。

【図１０】

実施形態のドアロック制御システムを構成するドアロック装置の一例の要部を説明するための図である。

【図１１】

図１０のドアロック装置のドアロック制御装置の構成例を示すブロック図である。

【図１２】

セキュリティシステムに用いる監視制御装置の例を示す図である。

【図１３】

図１２の監視制御装置の構成例を示すブロック図である。

【図１４】

個人プロファイル情報の一例を示す図である。

【図１５】

セキュリティモードの内容を説明するための図である。

【図１６】

セキュリティモードの内容を説明するための図である。

【図１７】

管理サーバ装置の構成例を示すブロック図である。

【図１８】

図１２の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

【図１９】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図２０】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図２１】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２２】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２３】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制

御動作を説明するためのフローチャートの一部である。

【図２４】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２５】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２６】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２７】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２８】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２９】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図３０】

監視制御装置のリモートコマンダからの信号の受信処理動作を説明するためのフローチャートである。

【図３１】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図３２】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図３３】

監視制御装置におけるドアロック装置との連携動作を説明するための図である。

【図３４】

この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

【図３５】

この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

【図３６】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのシステム構成を示す図である。

【図３７】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図３８】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図３９】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図４０】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合のシステム構成を説明するための図である。

【図４１】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順の一例を説明するための図である。

【図４２】

図４１の例における紛失鍵情報の抹消処理を説明するためのフローチャートを示す図である。

【図４３】

図４１の例における紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【図４４】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順の他の例を説明するための図である。

【図４５】

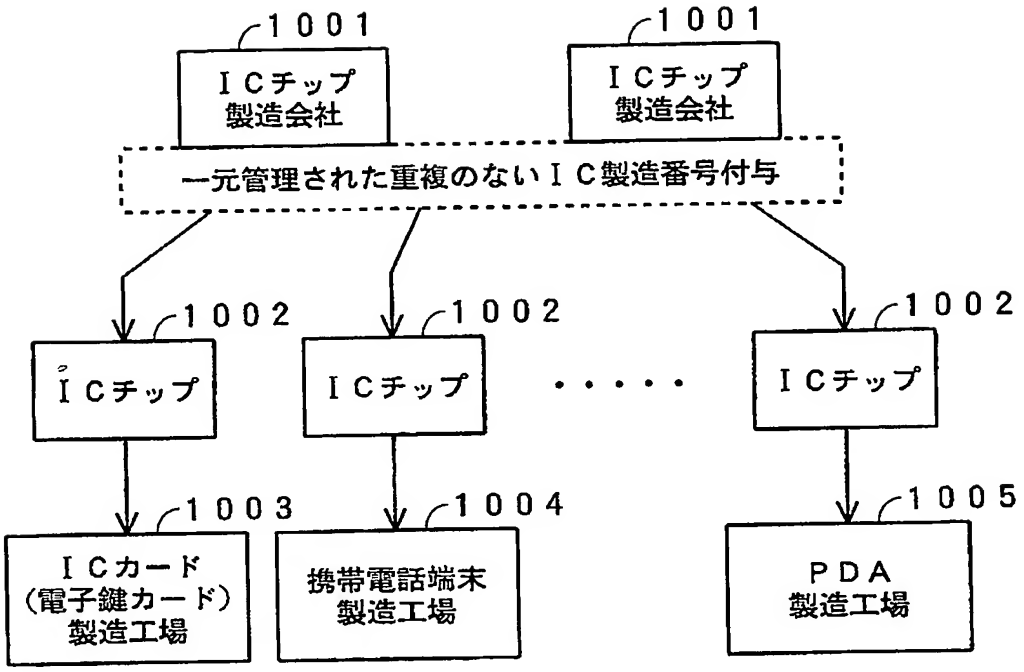
図４４の例における紛失鍵情報の抹消処理を説明するためのフローチャートを示す図である。

【符号の説明】

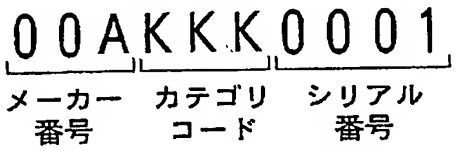
１…玄関ドア、２…ドアロック装置、３…監視制御装置、４…火災センサ、５…ガスセンサ、６ａ，６ｂ…窓センサ、７…テレビ受像機、８…電話回線、１０…管理サーバ装置、１００…ドアロック制御装置、２１ｉｎ…内側電子鍵リード／ライト部、２１ｅｘ…外側電子鍵リード／ライト部、４０Ｆ、４０Ｉ…電子鍵装置の例としてのＩＣカード

【書類名】　図面

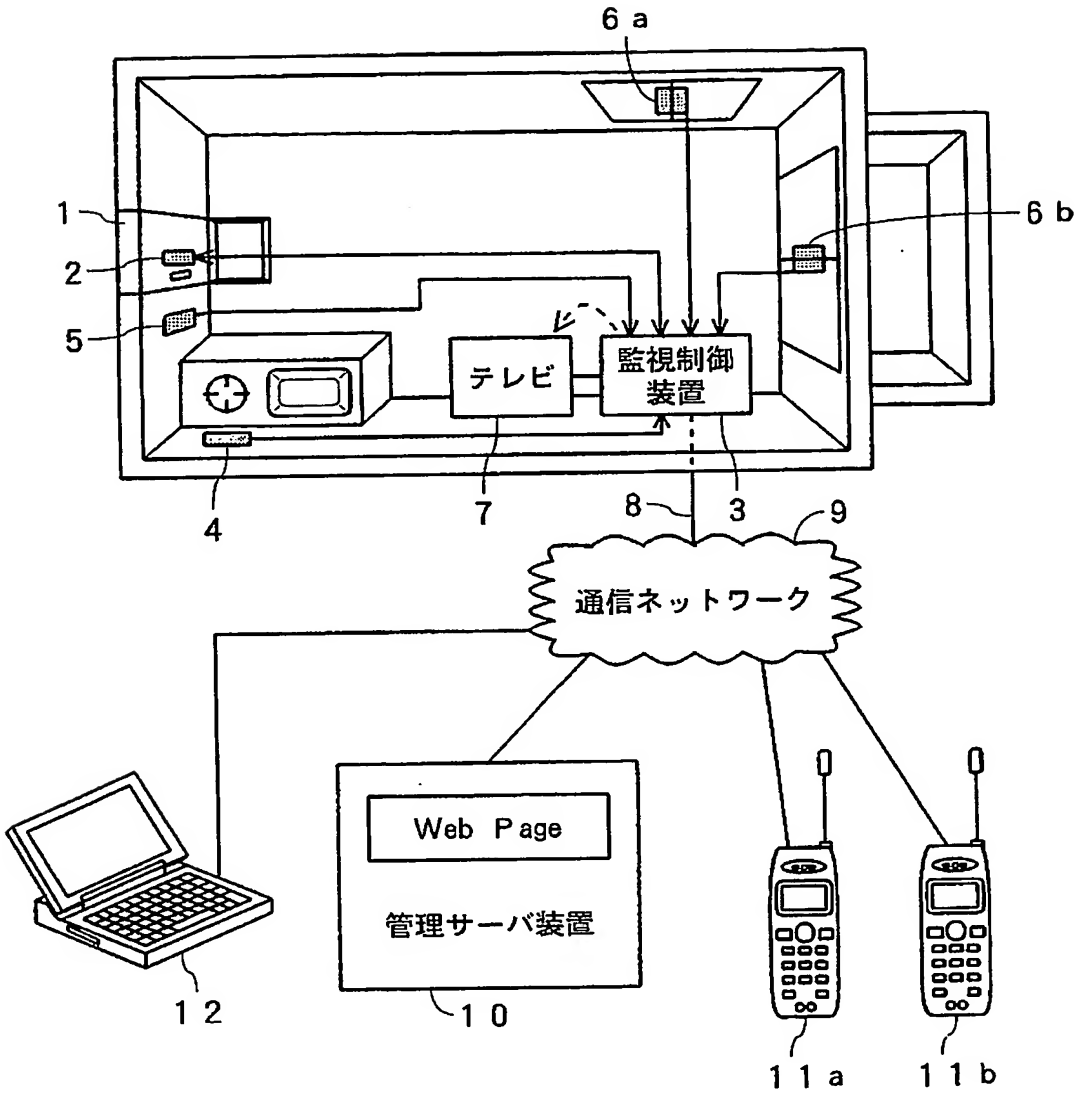
【図１】


1001
ＩＣチップ
製造会社
1001
ＩＣチップ
製造会社
一元管理された重複のないＩＣ製造番号付与
1002
ＩＣチップ
1002
ＩＣチップ
・・・・・
1002
ＩＣチップ
1003
ＩＣカード
（電子鍵カード）
製造工場
1004
携帯電話端末
製造工場
1005
ＰＤＡ
製造工場

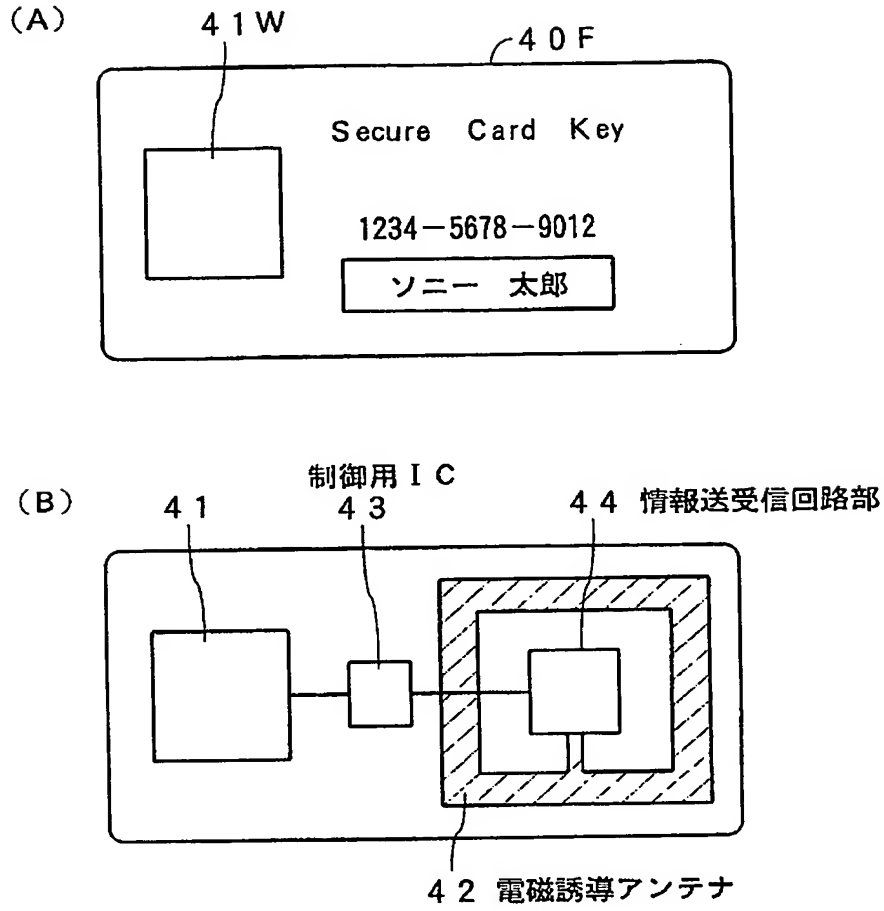
【図２】


００ＡＫＫ０００１
メーカー
番号
カテゴリ
コード
シリアル
番号

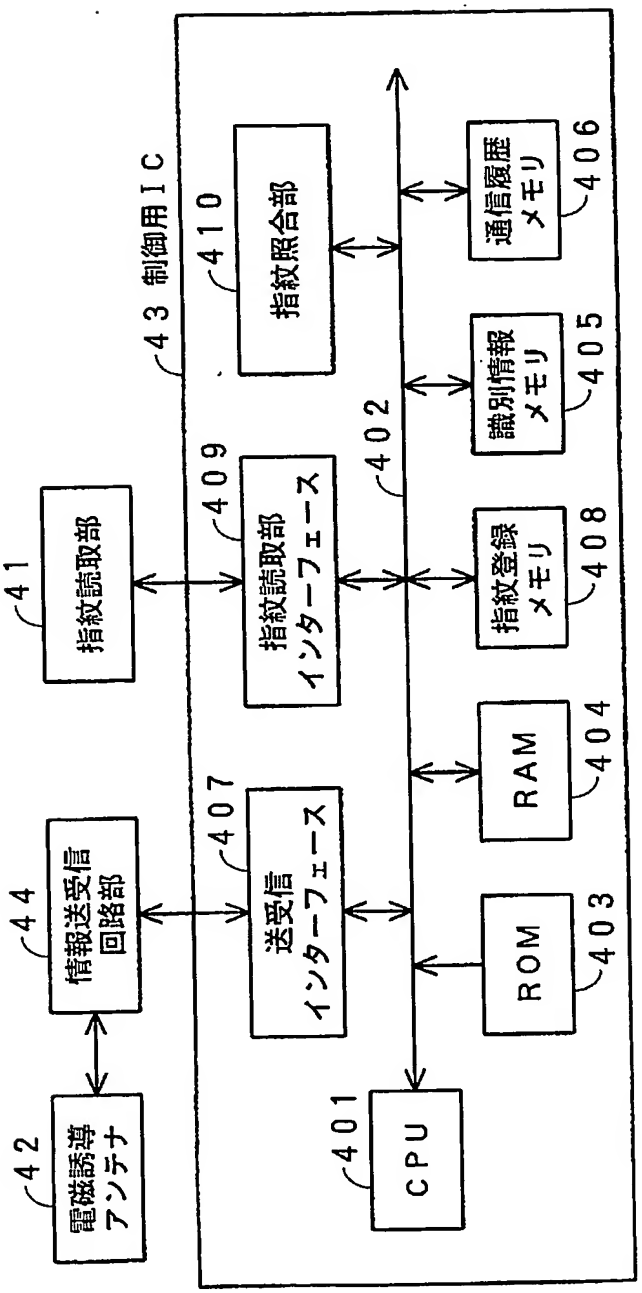
【図３】


6 a
1
2
5
6 b
テレビ
監視制御装置
4
7
8
3
9
通信ネットワーク
Web Page
管理サーバ装置
１２
１０
１１ａ
１１ｂ

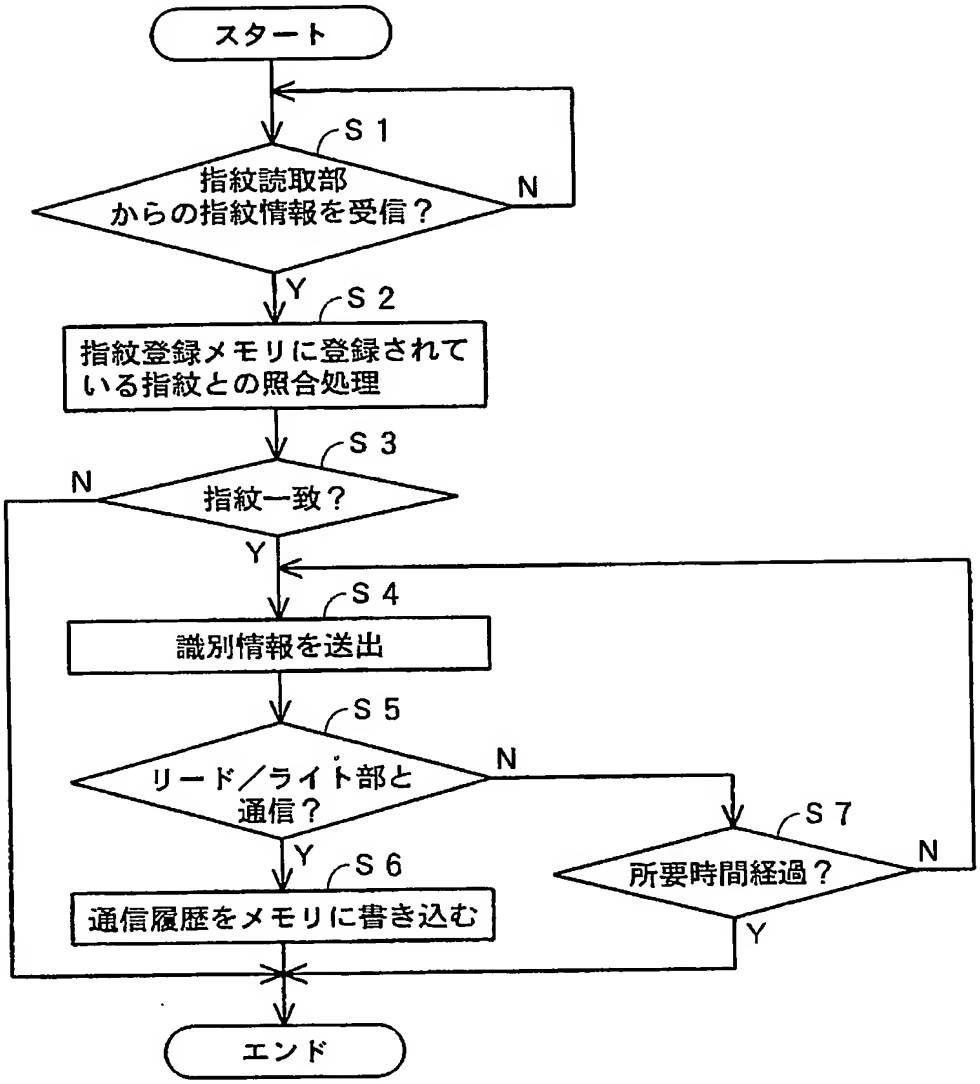
【図４】


（A）
４１Ｗ
４０Ｆ
Secure Card Key
1234－5678－9012
ソニー　太郎
（B）
制御用ＩＣ
４１
４３
４４　情報送受信回路部
４２　電磁誘導アンテナ

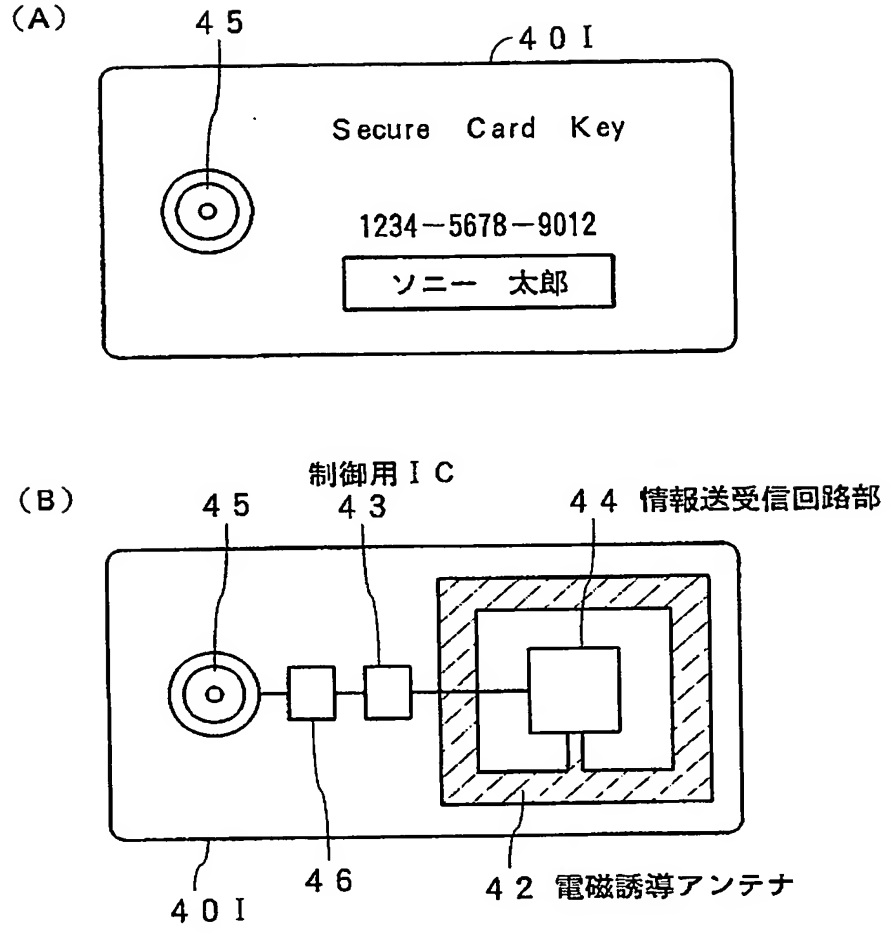
【図５】


43 制御用ＩＣ
41 指紋読取部
409 指紋読取部インターフェース
410 指紋照合部
402
406 通信履歴メモリ
405 識別情報メモリ
408 指紋登録メモリ
404 RAM
403 ROM
401 CPU
407 送受信インターフェース
44 情報送受信回路部
42 電磁誘導アンテナ

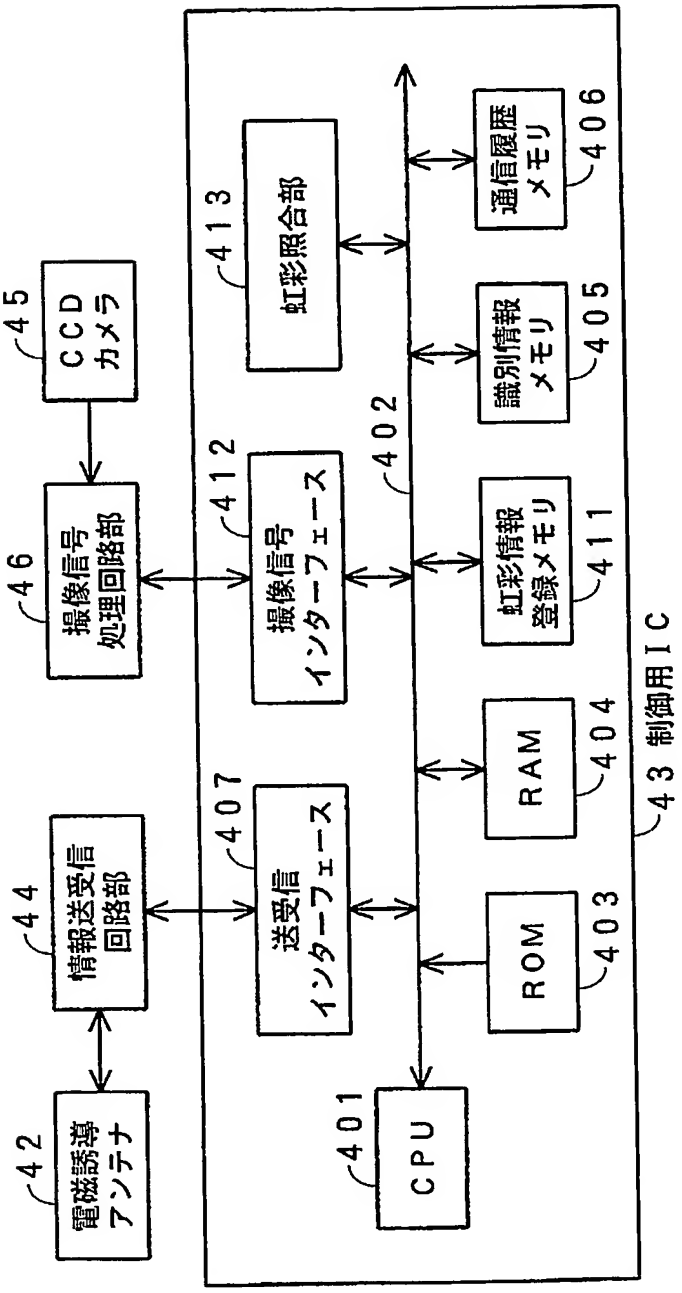
【図６】


スタート
S１
指紋読取部からの指紋情報を受信？
N
Y
S２
指紋登録メモリに登録されている指紋との照合処理
S３
指紋一致？
N
Y
S４
識別情報を送出
S５
リード／ライト部と通信？
N
Y
S６
通信履歴をメモリに書き込む
S７
所要時間経過？
N
Y
エンド

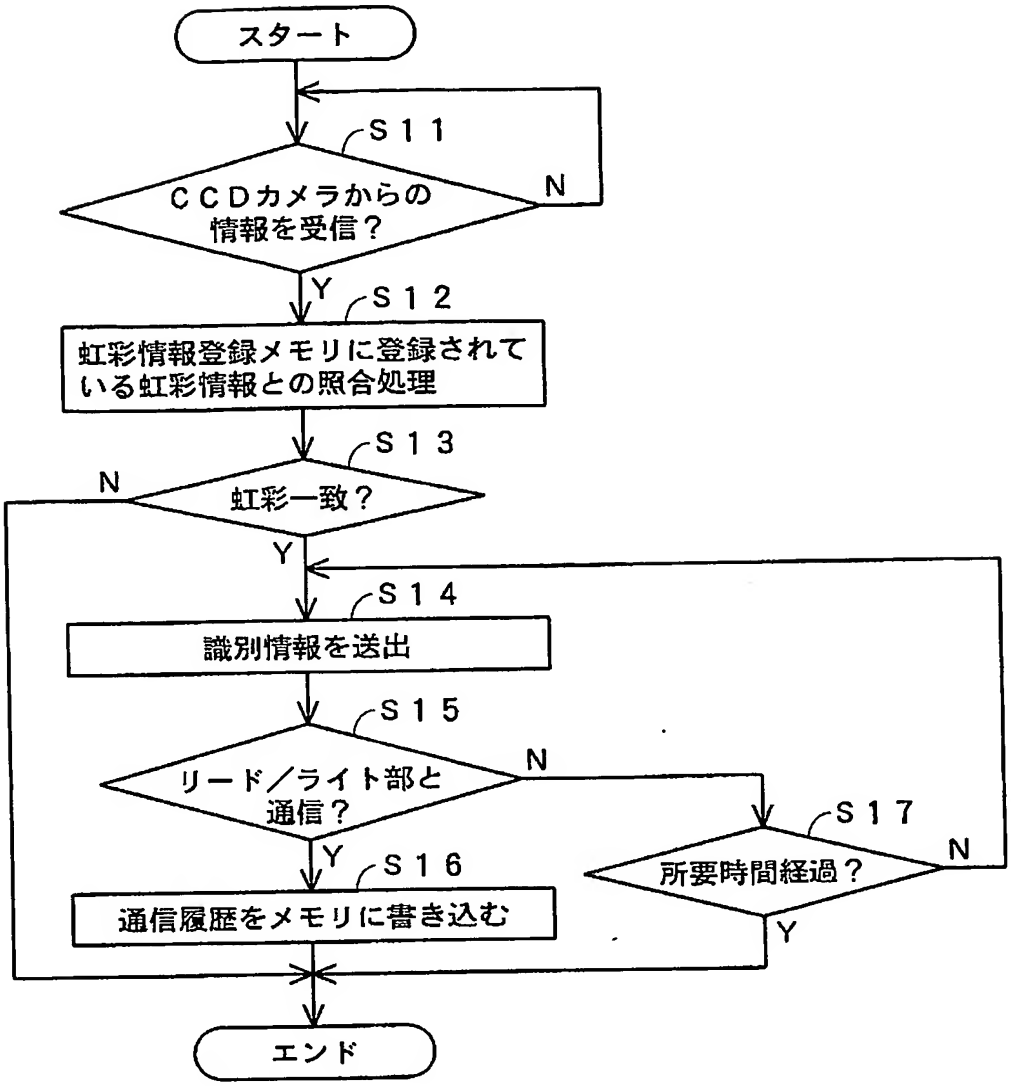
【図７】


(A)
４５
４０Ｉ
Secure Card Key
1234－5678－9012
ソニー　太郎
(B)
制御用ＩＣ
４３
４５
４４ 情報送受信回路部
４６
４０Ｉ
４２ 電磁誘導アンテナ

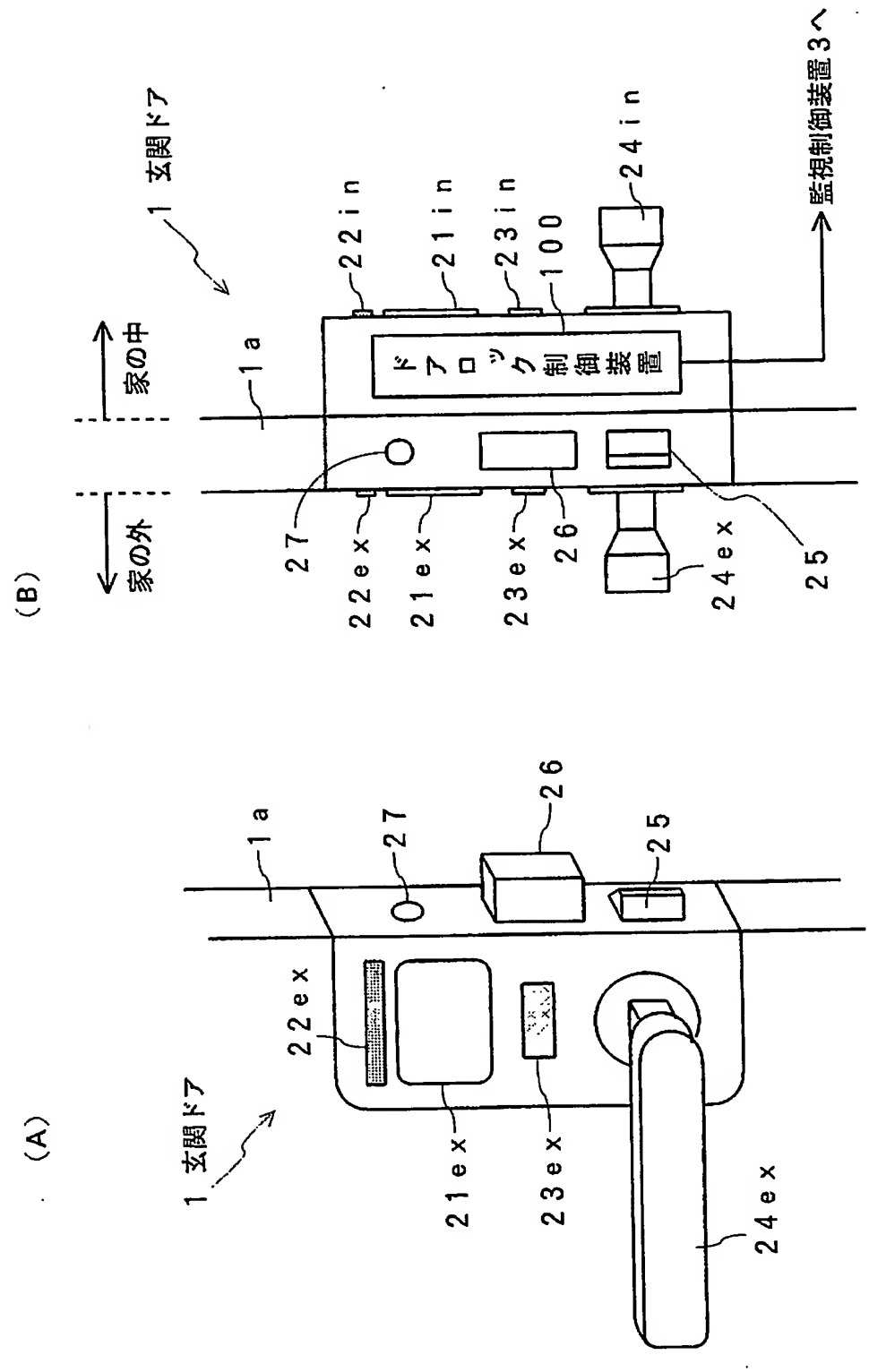
【図８】


４２
電磁誘導アンテナ
４４
情報送受信回路部
４６
撮像信号処理回路部
４５
ＣＣＤカメラ
４０７
送受信インターフェース
４１２
撮像信号インターフェース
４１３
虹彩照合部
４０２
４０１
ＣＰＵ
ＲＯＭ
４０３
ＲＡＭ
４０４
虹彩情報登録メモリ
４１１
識別情報メモリ
４０５
通信履歴メモリ
４０６
４３ 制御用ＩＣ

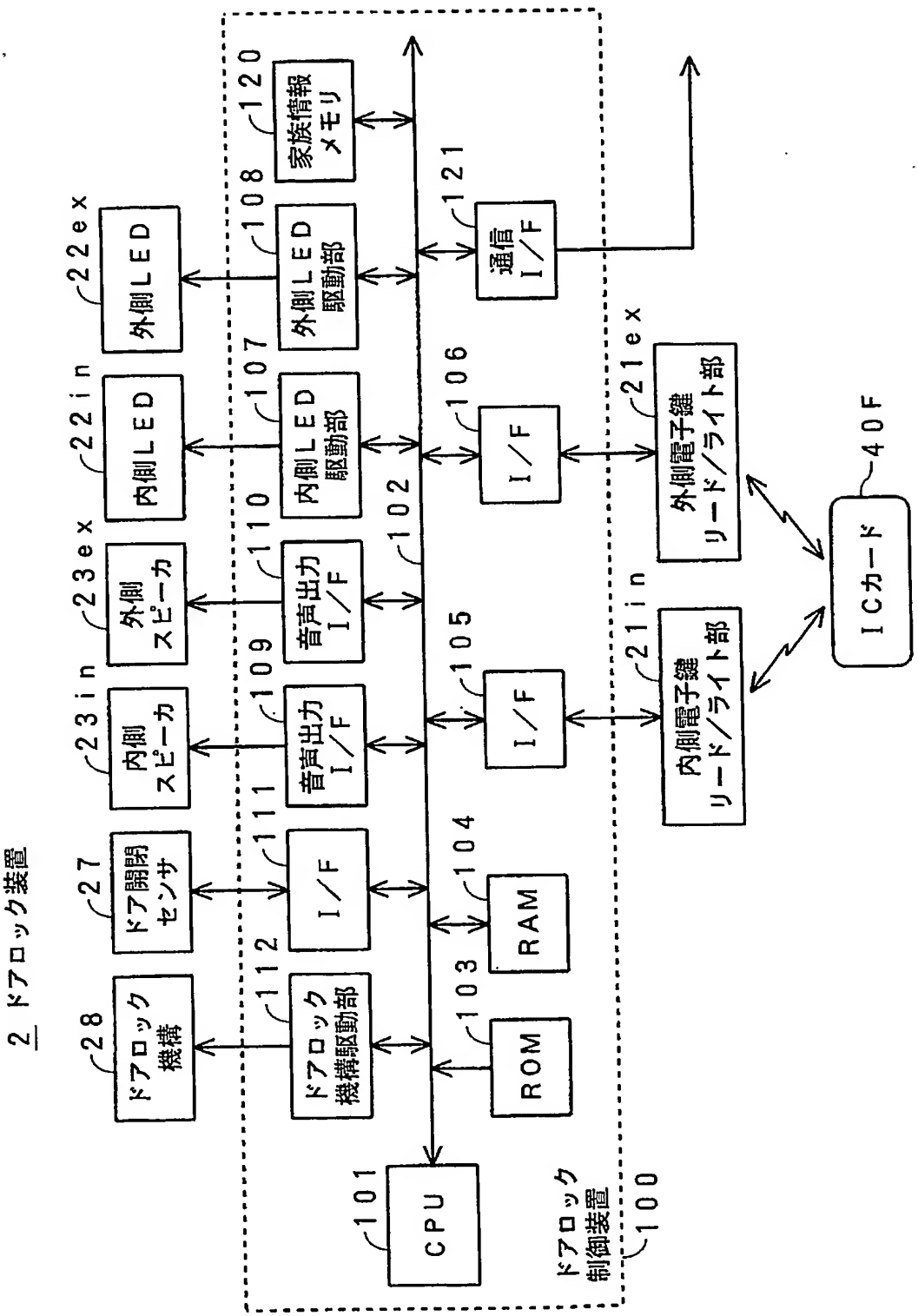
【図９】


スタート
S１１
ＣＣＤカメラからの情報を受信？
N
Y
S１２
虹彩情報登録メモリに登録されている虹彩情報との照合処理
S１３
虹彩一致？
N
Y
S１４
識別情報を送出
S１５
リード／ライト部と通信？
N
Y
S１６
通信履歴をメモリに書き込む
S１７
所要時間経過？
N
Y
エンド

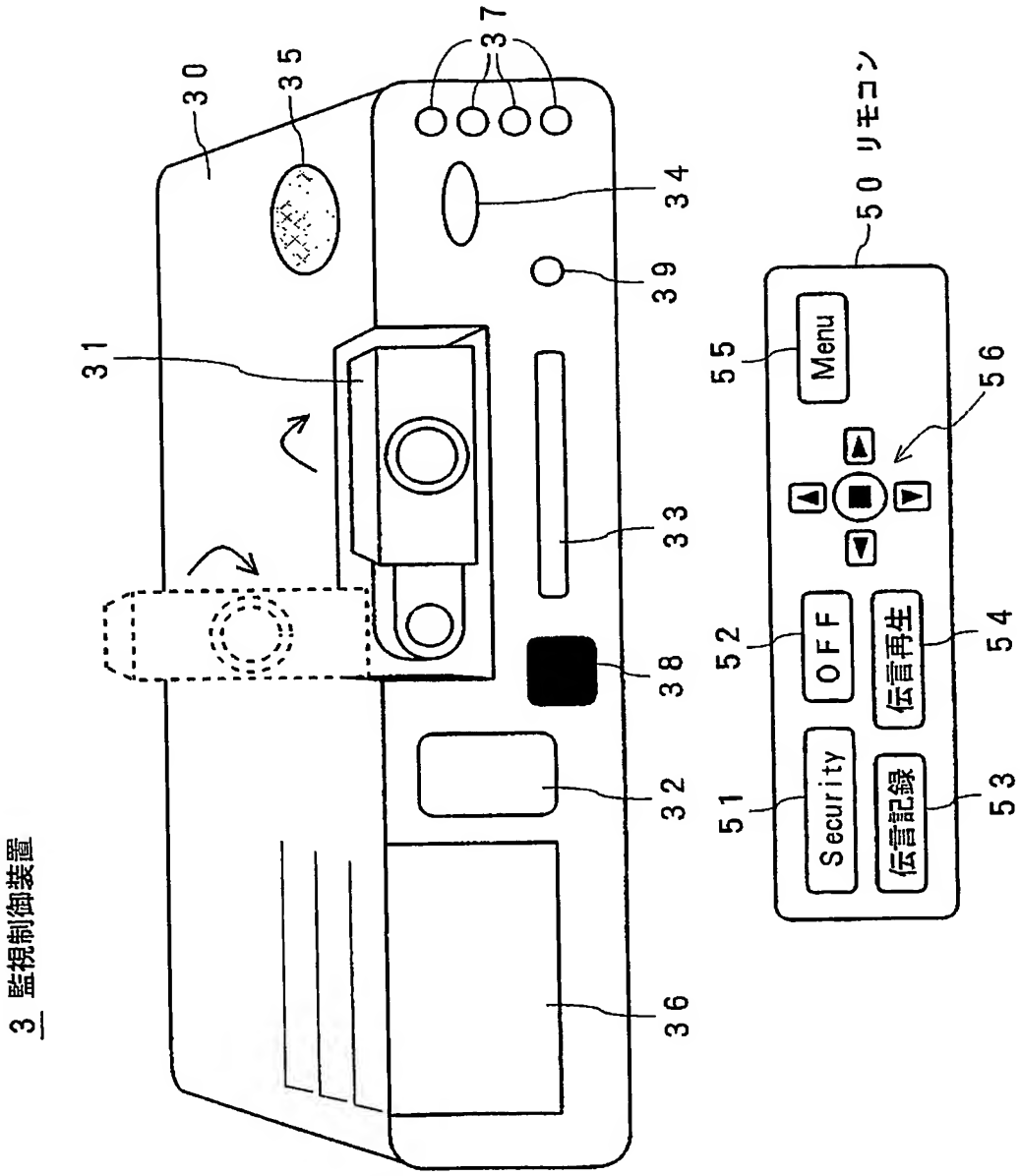
【図１０】


(A)
2 ドアロック装置
1 玄関ドア
1a
27
26
25
22ex
21ex
23ex
24ex
(B)
1 玄関ドア
家の中
家の外
1a
22in
21in
23in
100
24in
ドアロック制御装置
監視制御装置3へ
27
22ex
21ex
23ex
26
24ex
25

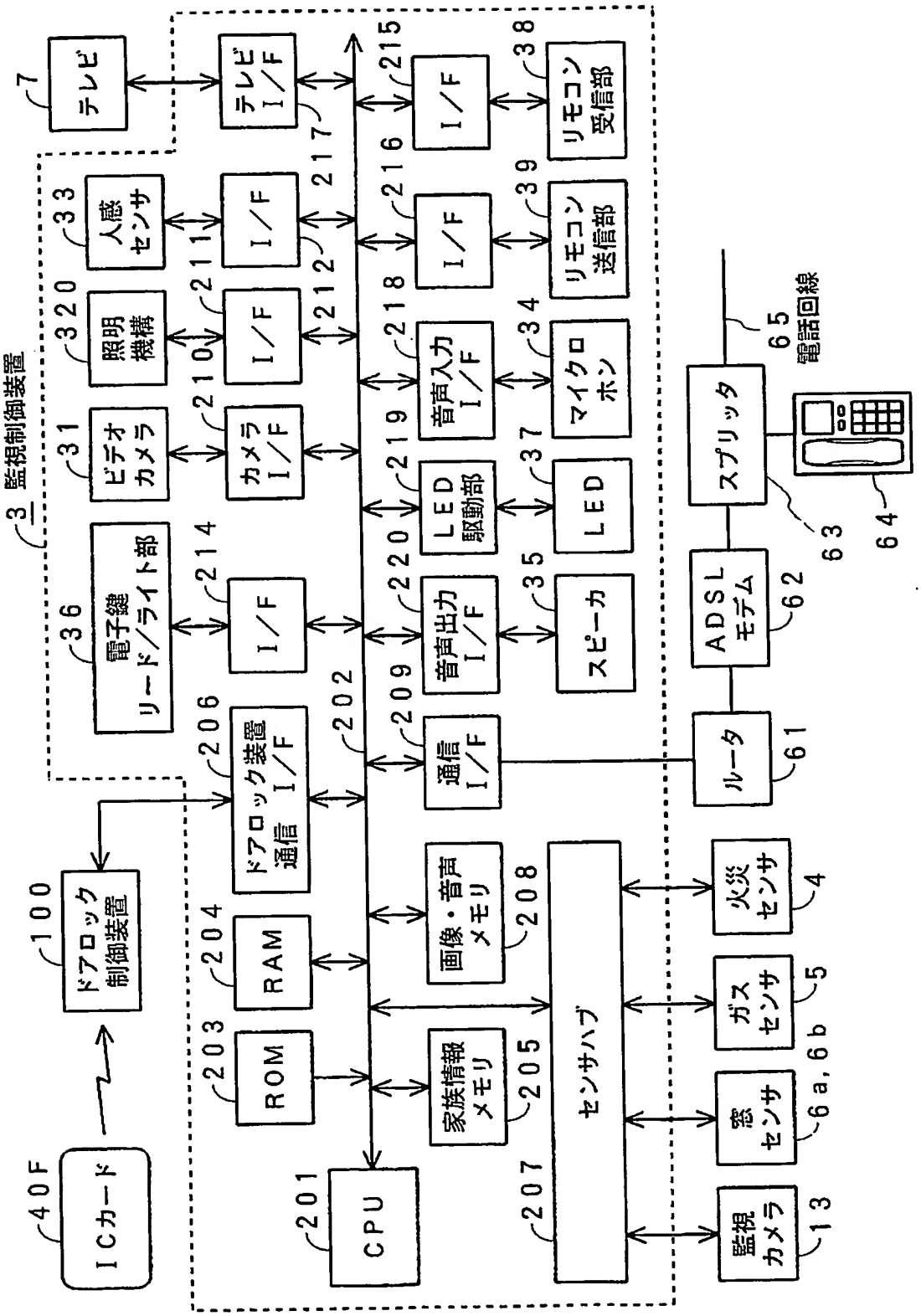
【図１１】


2 ドアロック装置
ドアロック制御装置
100
CPU
101
ROM
103
RAM
104
I／F
105
I／F
106
I／F
111
I／F
112
ドアロック機構駆動部
28
ドアロック機構
ドア開閉センサ
27
内側スピーカ
23in
外側スピーカ
23ex
内側LED
22in
外側LED
22ex
音声出力I／F
109
音声出力I／F
110
内側LED駆動部
107
外側LED駆動部
108
家族情報メモリ
120
通信I／F
121
内側電子鍵リード／ライト部
21in
外側電子鍵リード／ライト部
21ex
ICカード
40F

【図１２】


3 監視制御装置
30
35
37
34
39
31
33
38
32
36
50 リモコン
55
Menu
56
52
OFF
伝言再生
54
51
Security
伝言記録
53

【図１３】


3 監視制御装置
7 テレビ
テレビ I／F
215
I／F
38 リモコン 受信部
33 人感 センサ
I／F
211
217
216
I／F
39 リモコン 送信部
320 照明 機構
I／F
210
212
218
I／F
34 マイクロ ホン
31 ビデオ カメラ
カメラ I／F
219
音声入力 I／F
37 LED
214
LED 駆動部
220
35 スピーカ
36 電子鍵 リード／ライト部
I／F
音声出力 I／F
209
206
202
ドアロック装置 通信 I／F
通信 I／F
61 ルータ
ADSL モデム
62
スプリッタ
63
65 電話回線
64
100 ドアロック 制御装置
204 RAM
画像・音声 メモリ
208
火災 センサ
4
203 ROM
家族情報 メモリ
205
センサハブ
ガス センサ
5
40F ICカード
201 CPU
207
窓 センサ
6a, 6b
監視 カメラ
13

【図１４】

個人プロファイル情報

	識別情報 ・本鍵情報 ・バックアップ鍵情報	個人識別情報
	パスワード情報	個人情報
	氏名	
	住所	
	生年月日	
	年齢	
	続柄	
	登録日	
	銀行口座番号	
	電話番号	
	ＩＰアドレス	
	趣味／嗜好情報 ・好きなテレビ番組：ドラマ ・好きな音楽：ジャズ ・好きな映画：ＳＦ	
	入退出履歴情報	
	電子鍵登録・紛失履歴情報	

【図１５】

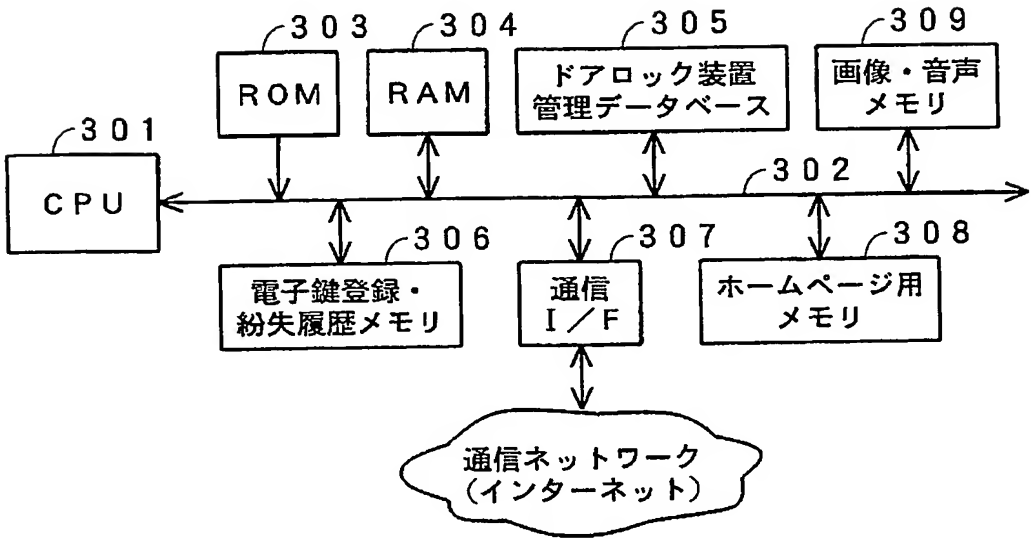
セキュリティレベル	父親	母親	子供
D	○	○	○
D	○	○	×
D	○	×	○
D	○	×	×
C	×	○	○
C	×	○	×
B	×	×	○
A	×	×	×

○：在宅
×：不在

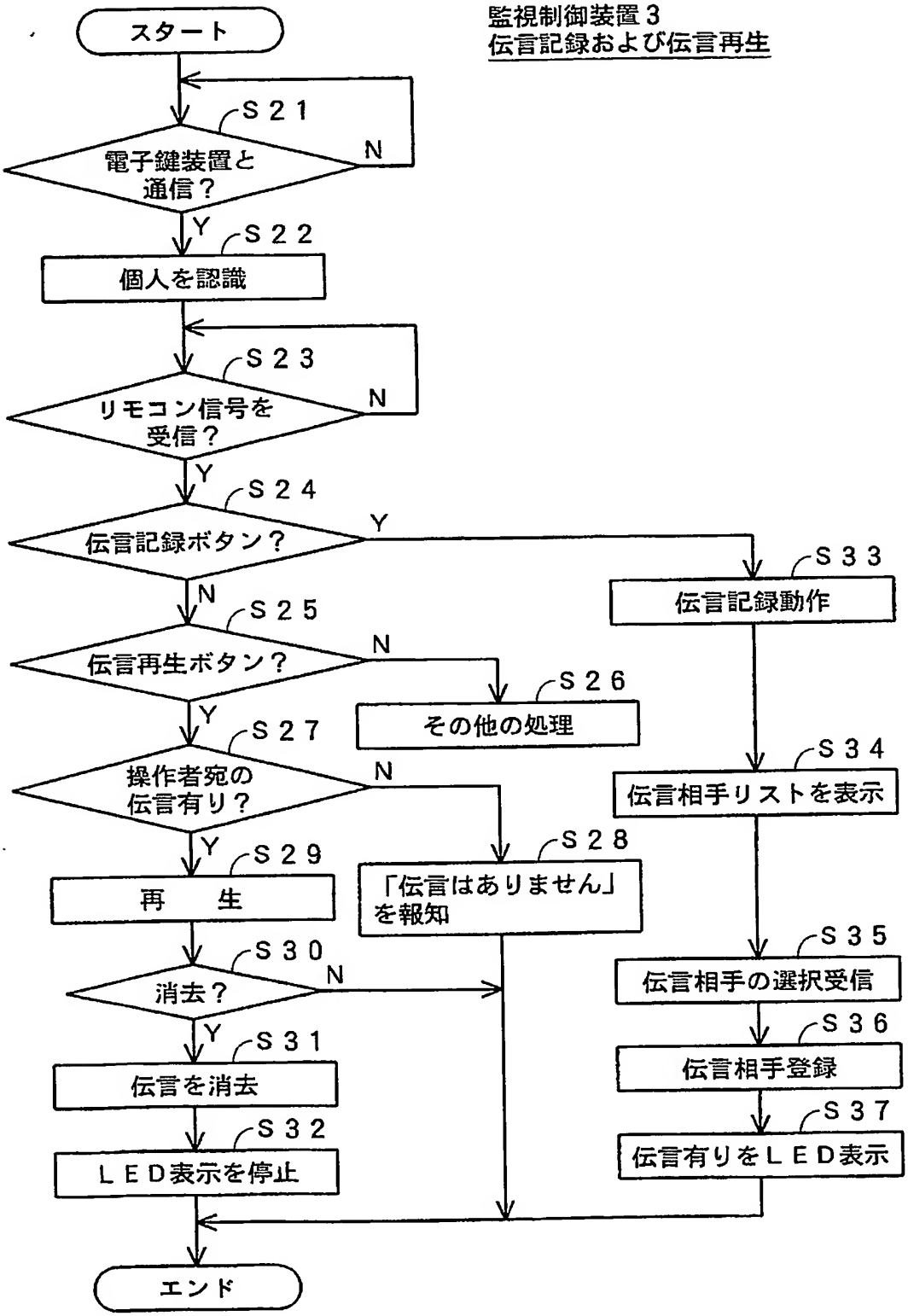
【図１６】

セキュリティレベル	窓・ドア監視	火災・ガス監視	カメラ監視
A	○	○	○
B	○	○	×
C	×	○	×
D	×	×	×

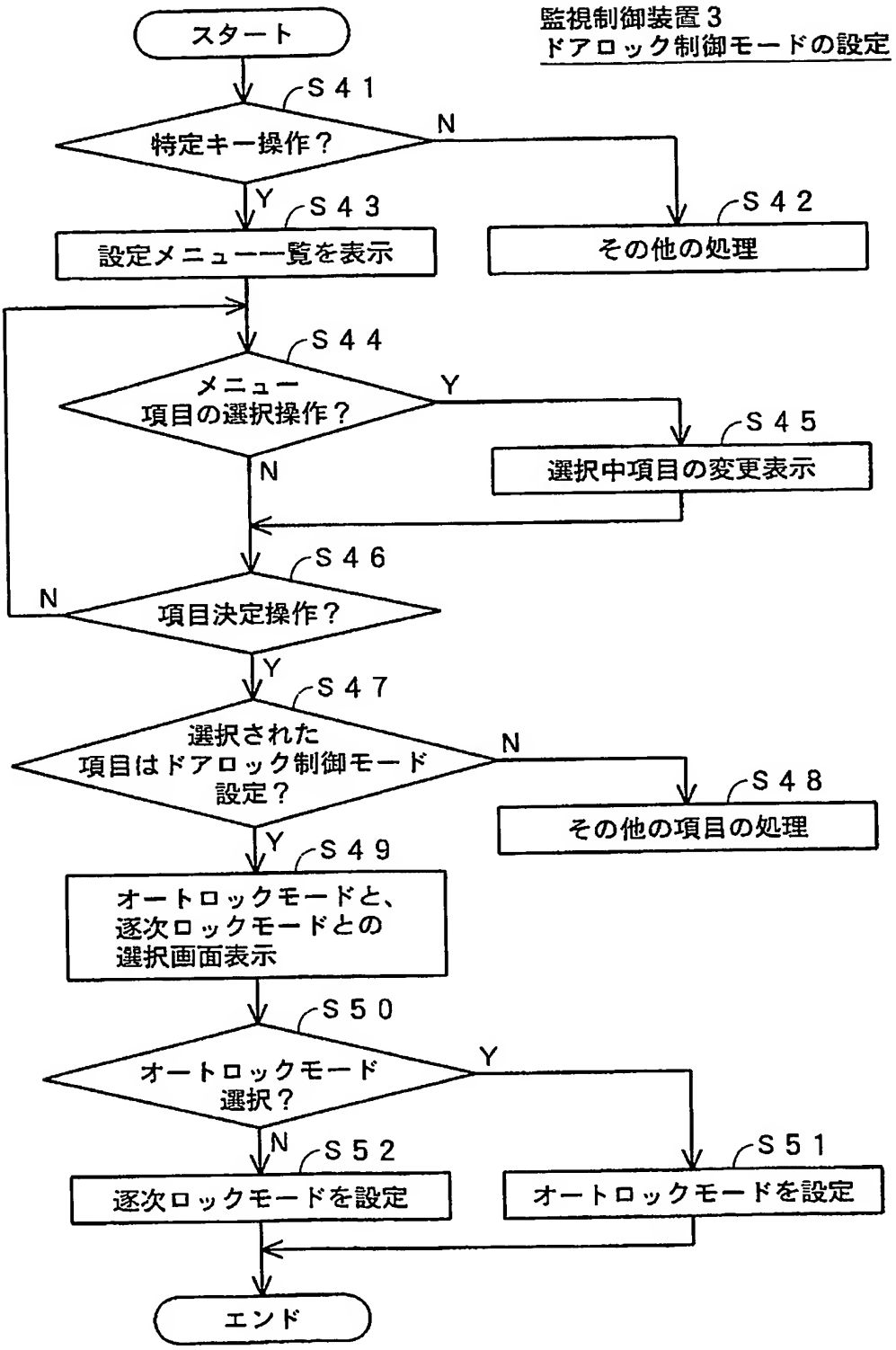
【図１７】


１０ 管理サーバ装置
３０３
ROM
３０４
RAM
３０５
ドアロック装置
管理データベース
３０９
画像・音声
メモリ
３０１
CPU
３０２
３０６
電子鍵登録・
紛失履歴メモリ
３０７
通信
Ｉ／Ｆ
３０８
ホームページ用
メモリ
通信ネットワーク
（インターネット）

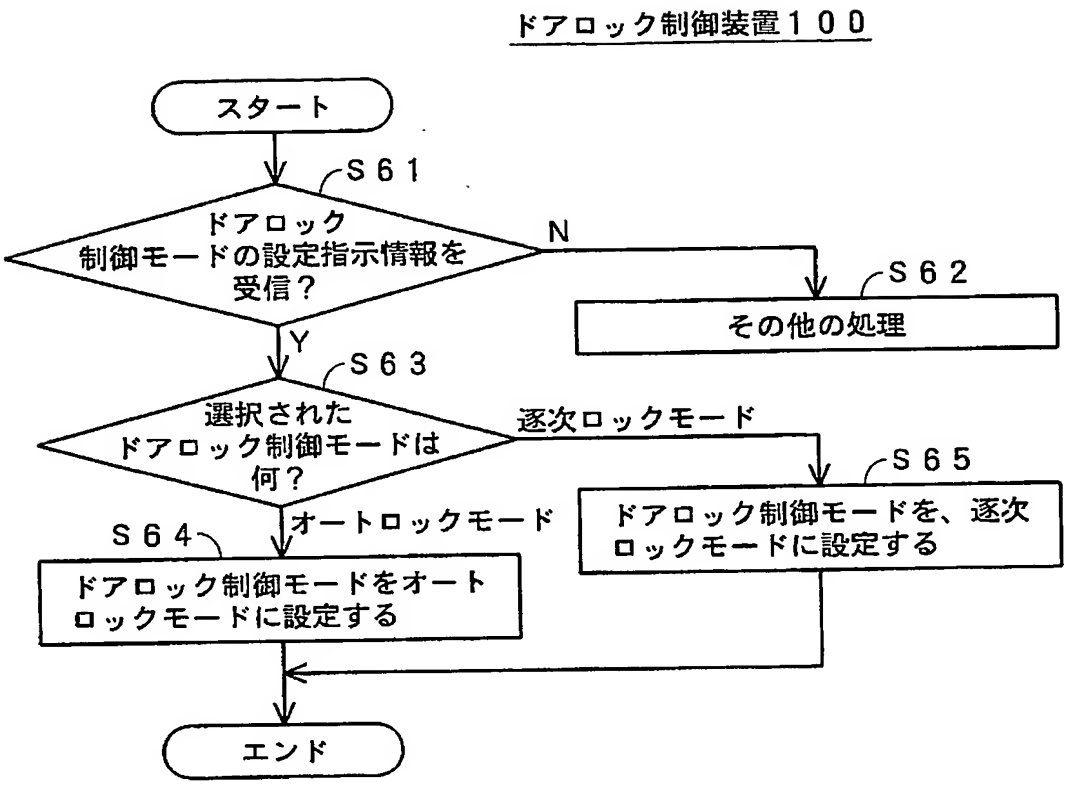
【図１８】


監視制御装置３
伝言記録および伝言再生
スタート
Ｓ２１
電子鍵装置と通信？
N
Y
Ｓ２２
個人を認識
Ｓ２３
リモコン信号を受信？
N
Y
Ｓ２４
伝言記録ボタン？
Y
N
Ｓ２５
伝言再生ボタン？
N
Y
Ｓ２６
その他の処理
Ｓ２７
操作者宛の伝言有り？
N
Y
Ｓ２８
「伝言はありません」を報知
Ｓ２９
再　生
Ｓ３０
消去？
N
Y
Ｓ３１
伝言を消去
Ｓ３２
ＬＥＤ表示を停止
エンド
Ｓ３３
伝言記録動作
Ｓ３４
伝言相手リストを表示
Ｓ３５
伝言相手の選択受信
Ｓ３６
伝言相手登録
Ｓ３７
伝言有りをＬＥＤ表示

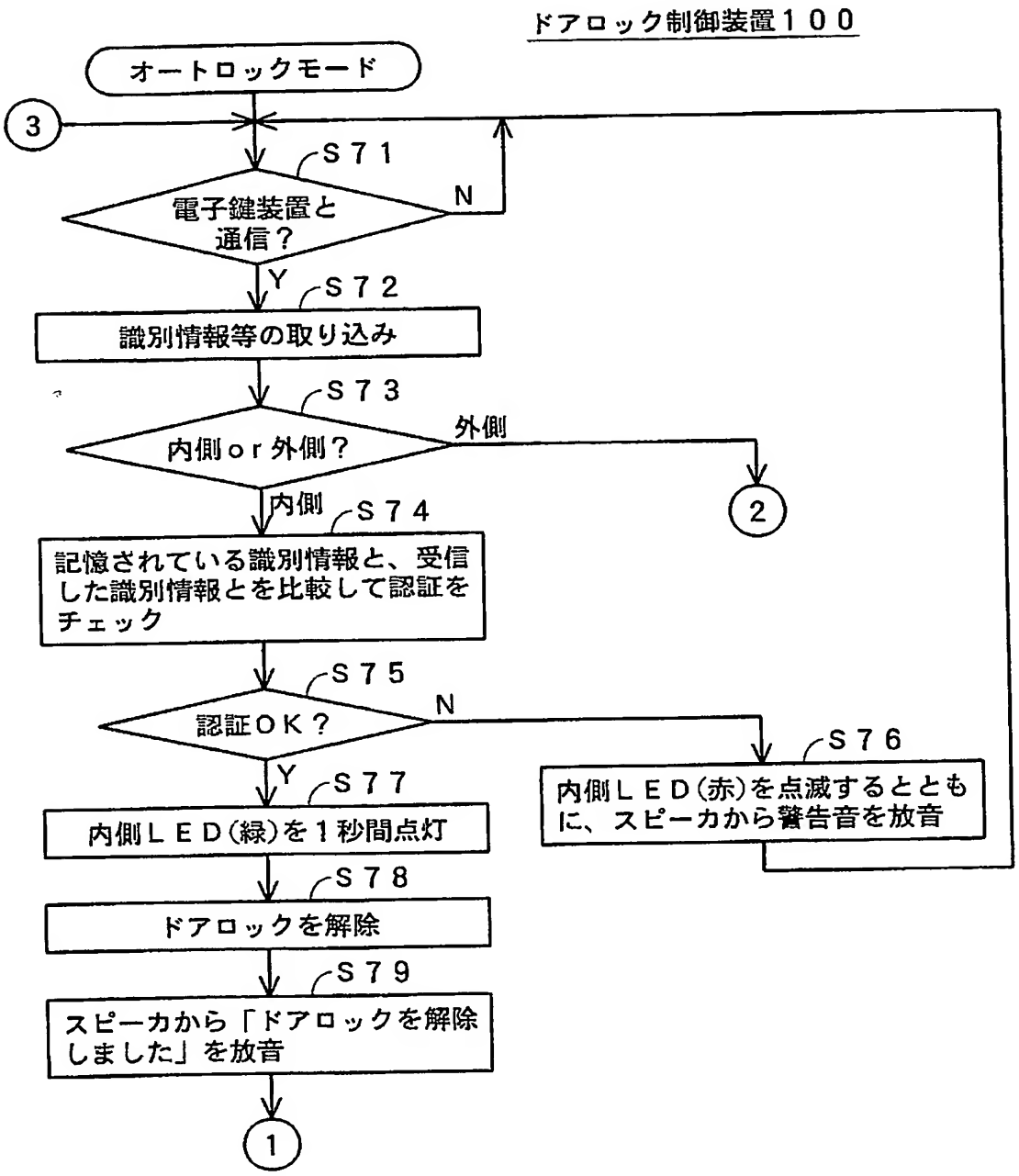
【図１９】


監視制御装置３
ドアロック制御モードの設定
スタート
Ｓ４１
特定キー操作？
N
Y
Ｓ４３
設定メニュー一覧を表示
Ｓ４２
その他の処理
Ｓ４４
メニュー
項目の選択操作？
Y
Ｓ４５
選択中項目の変更表示
N
Ｓ４６
項目決定操作？
N
Y
Ｓ４７
選択された
項目はドアロック制御モード
設定？
N
Ｓ４８
その他の項目の処理
Y
Ｓ４９
オートロックモードと、
逐次ロックモードとの
選択画面表示
Ｓ５０
オートロックモード
選択？
Y
N
Ｓ５２
逐次ロックモードを設定
Ｓ５１
オートロックモードを設定
エンド

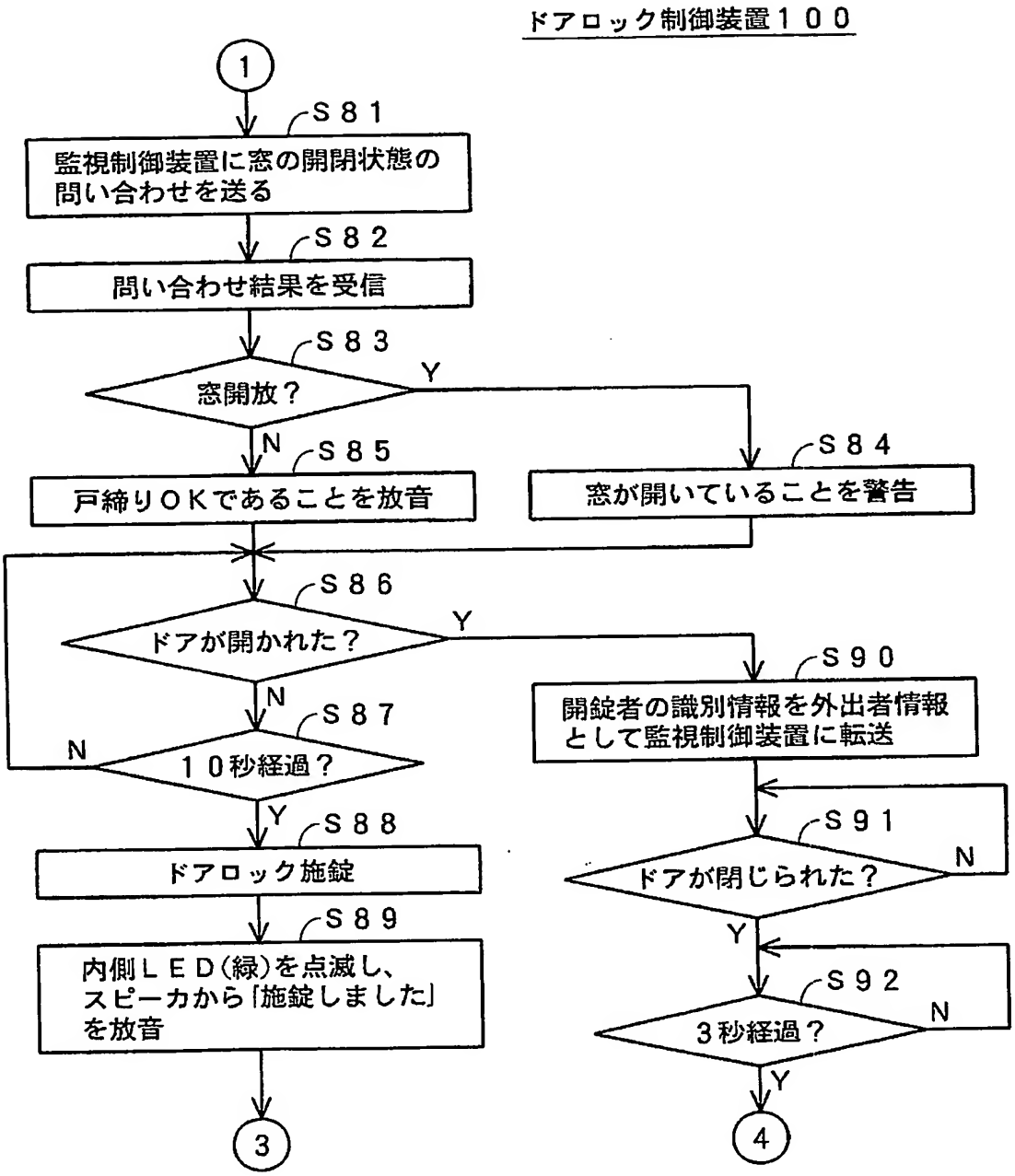
【図２０】


ドアロック制御装置１００
スタート
Ｓ６１
ドアロック制御モードの設定指示情報を受信？
N
Ｓ６２
その他の処理
Y
Ｓ６３
選択されたドアロック制御モードは何？
逐次ロックモード
Ｓ６５
ドアロック制御モードを、逐次ロックモードに設定する
オートロックモード
Ｓ６４
ドアロック制御モードをオートロックモードに設定する
エンド

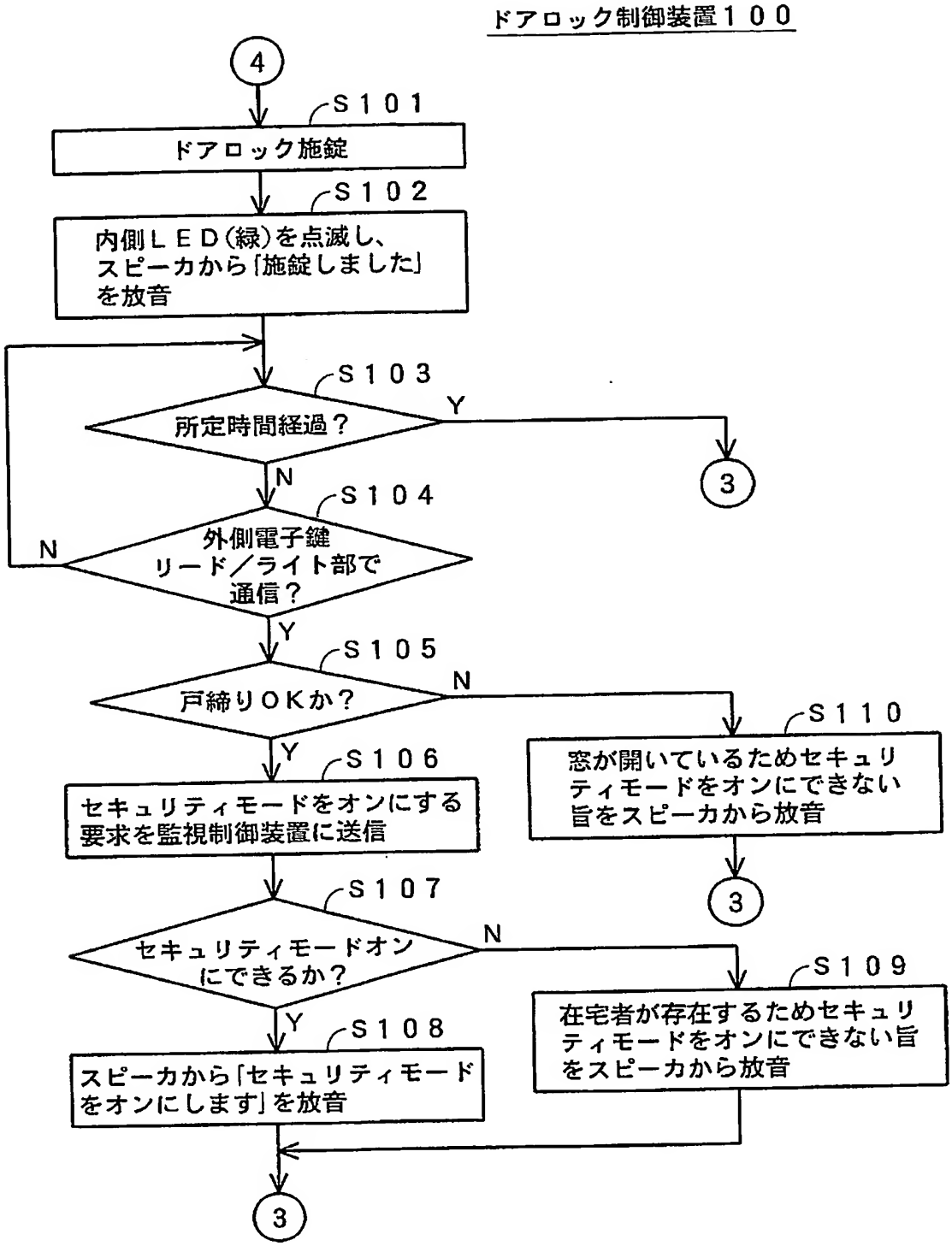
【図２１】


ドアロック制御装置１００
オートロックモード
3
S７１
電子鍵装置と通信？
N
Y
S７２
識別情報等の取り込み
S７３
内側ｏｒ外側？
外側
2
内側
S７４
記憶されている識別情報と、受信した識別情報とを比較して認証をチェック
S７５
認証ＯＫ？
N
S７６
内側ＬＥＤ(赤)を点滅するとともに、スピーカから警告音を放音
Y
S７７
内側ＬＥＤ(緑)を１秒間点灯
S７８
ドアロックを解除
S７９
スピーカから「ドアロックを解除しました」を放音
1

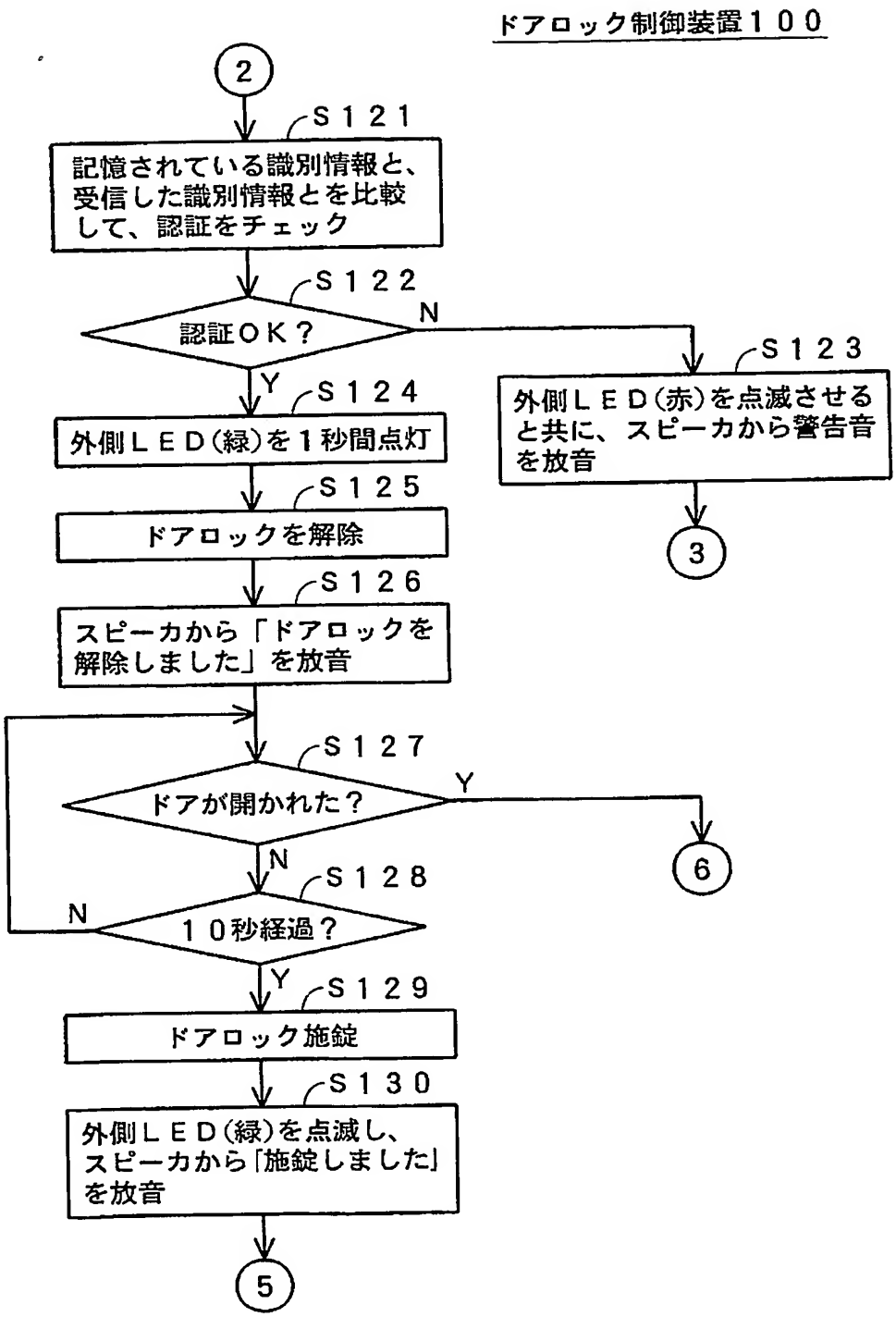
【図２２】


ドアロック制御装置１００
1
S８１
監視制御装置に窓の開閉状態の問い合わせを送る
S８２
問い合わせ結果を受信
S８３
窓開放？
Y
N
S８５
戸締りＯＫであることを放音
S８４
窓が開いていることを警告
S８６
ドアが開かれた？
Y
N
S８７
１０秒経過？
N
Y
S８８
ドアロック施錠
S８９
内側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
3
S９０
開錠者の識別情報を外出者情報として監視制御装置に転送
S９１
ドアが閉じられた？
N
Y
S９２
３秒経過？
N
Y
4

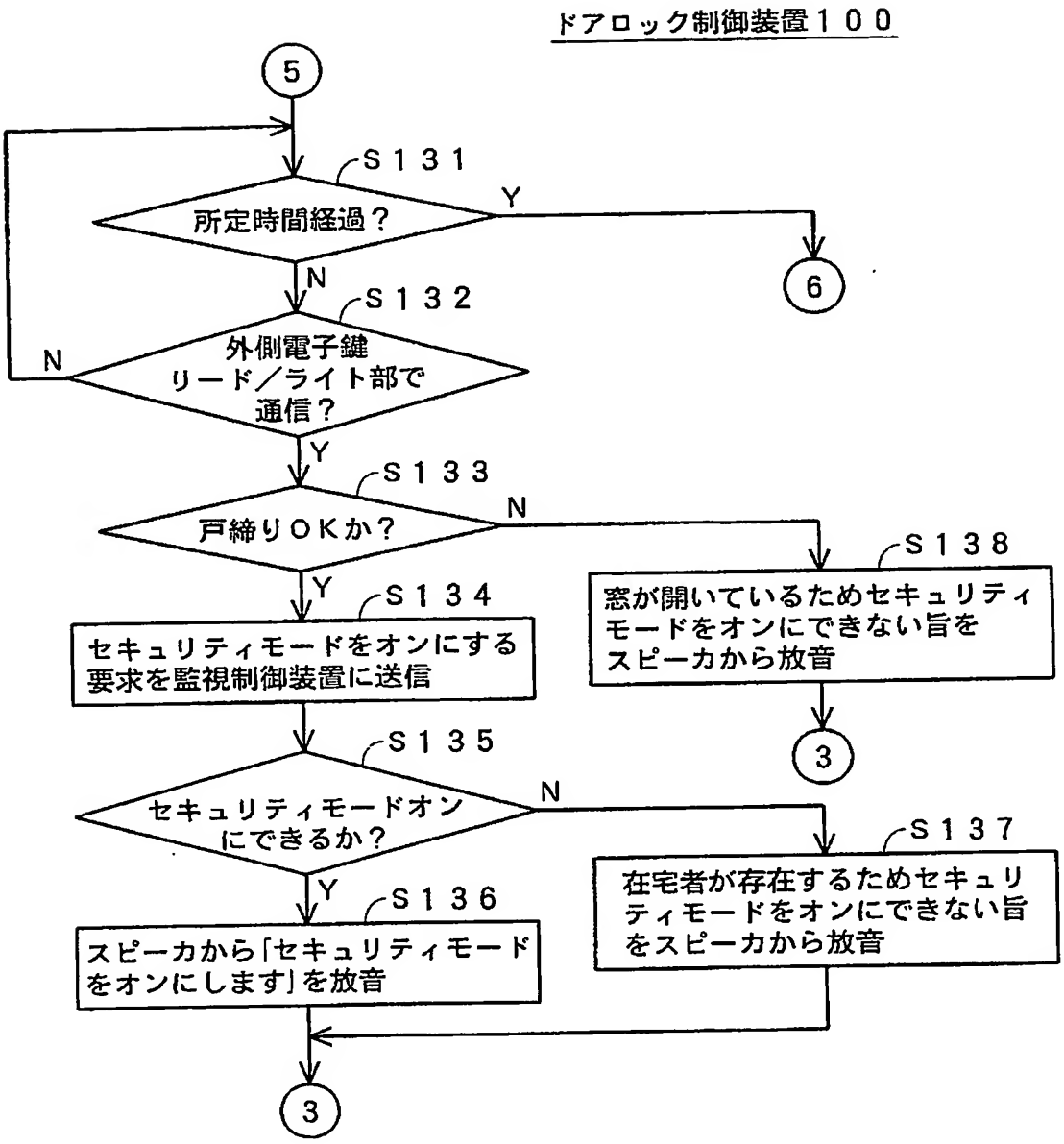
【図２３】


ドアロック制御装置１００
4
S１０１
ドアロック施錠
S１０２
内側ＬＥＤ(緑)を点滅し、
スピーカから「施錠しました」
を放音
S１０３
所定時間経過？
Y
N
3
S１０４
外側電子鍵
リード／ライト部で
通信？
N
Y
S１０５
戸締りＯＫか？
N
Y
S１１０
窓が開いているためセキュリ
ティモードをオンにできない
旨をスピーカから放音
S１０６
セキュリティモードをオンにする
要求を監視制御装置に送信
3
S１０７
セキュリティモードオン
にできるか？
N
Y
S１０９
在宅者が存在するためセキュリ
ティモードをオンにできない旨
をスピーカから放音
S１０８
スピーカから「セキュリティモード
をオンにします」を放音
3

【図２４】

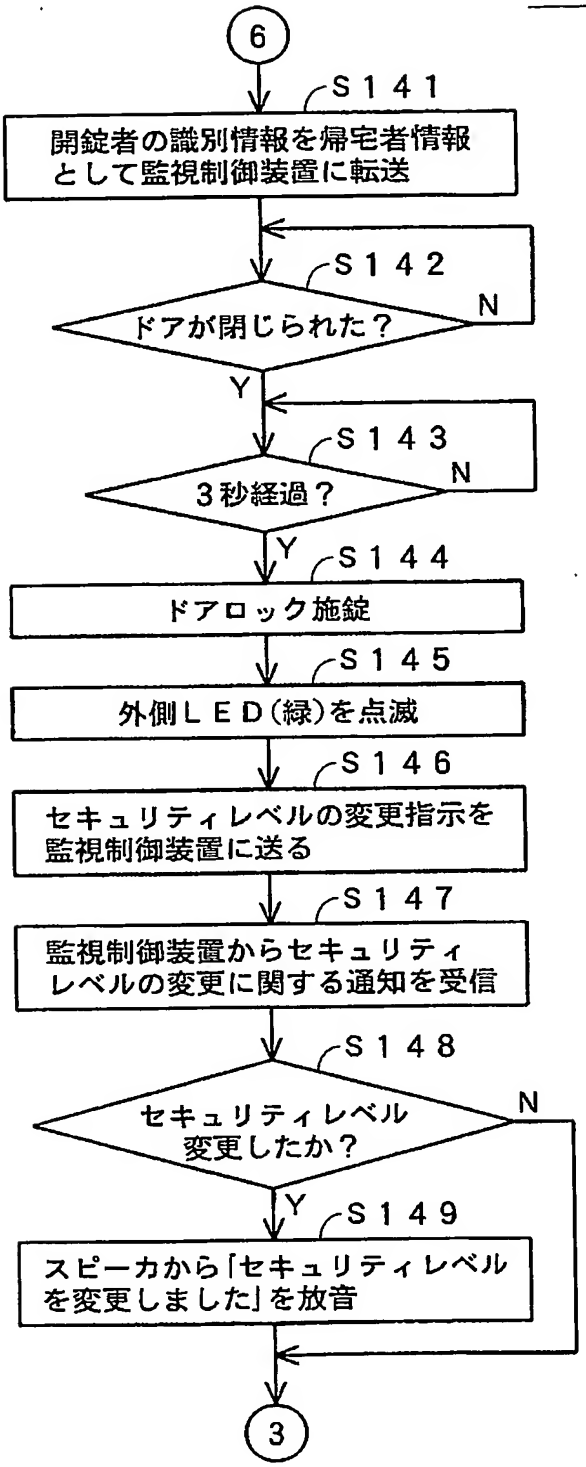

ドアロック制御装置１００
2
S１２１
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１２２
認証ＯＫ？
N
S１２３
外側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
3
Y
S１２４
外側ＬＥＤ(緑)を１秒間点灯
S１２５
ドアロックを解除
S１２６
スピーカから「ドアロックを解除しました」を放音
S１２７
ドアが開かれた？
Y
6
N
S１２８
１０秒経過？
N
Y
S１２９
ドアロック施錠
S１３０
外側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
5

【図２５】

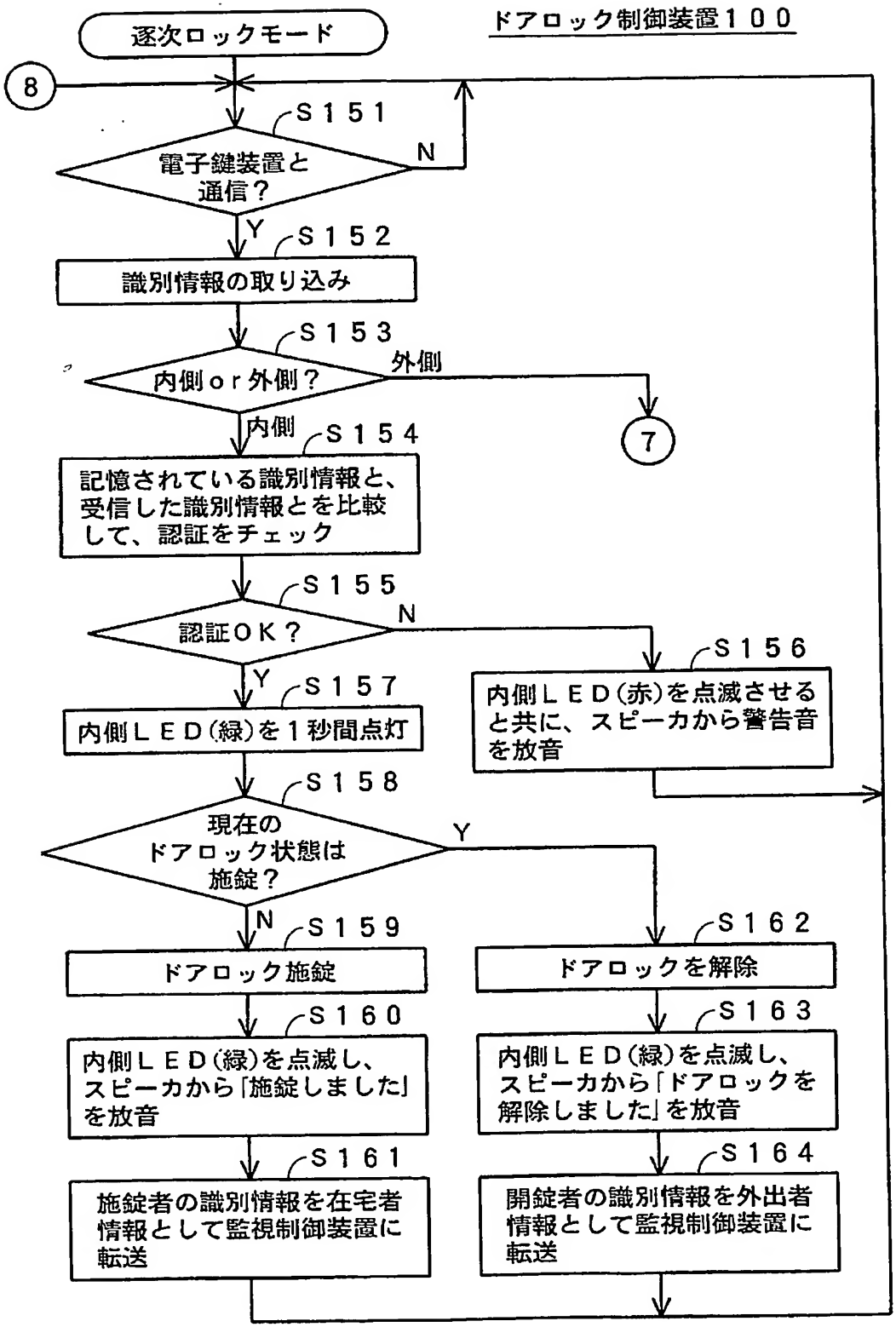

ドアロック制御装置１００
5
S１３１
所定時間経過？
Y
N
6
S１３２
外側電子鍵
リード／ライト部で
通信？
N
Y
S１３３
戸締りＯＫか？
N
Y
S１３８
窓が開いているためセキュリティ
モードをオンにできない旨を
スピーカから放音
3
S１３４
セキュリティモードをオンにする
要求を監視制御装置に送信
S１３５
セキュリティモードオン
にできるか？
N
Y
S１３７
在宅者が存在するためセキュリ
ティモードをオンにできない旨
をスピーカから放音
S１３６
スピーカから「セキュリティモード
をオンにします」を放音
3

【図２６】

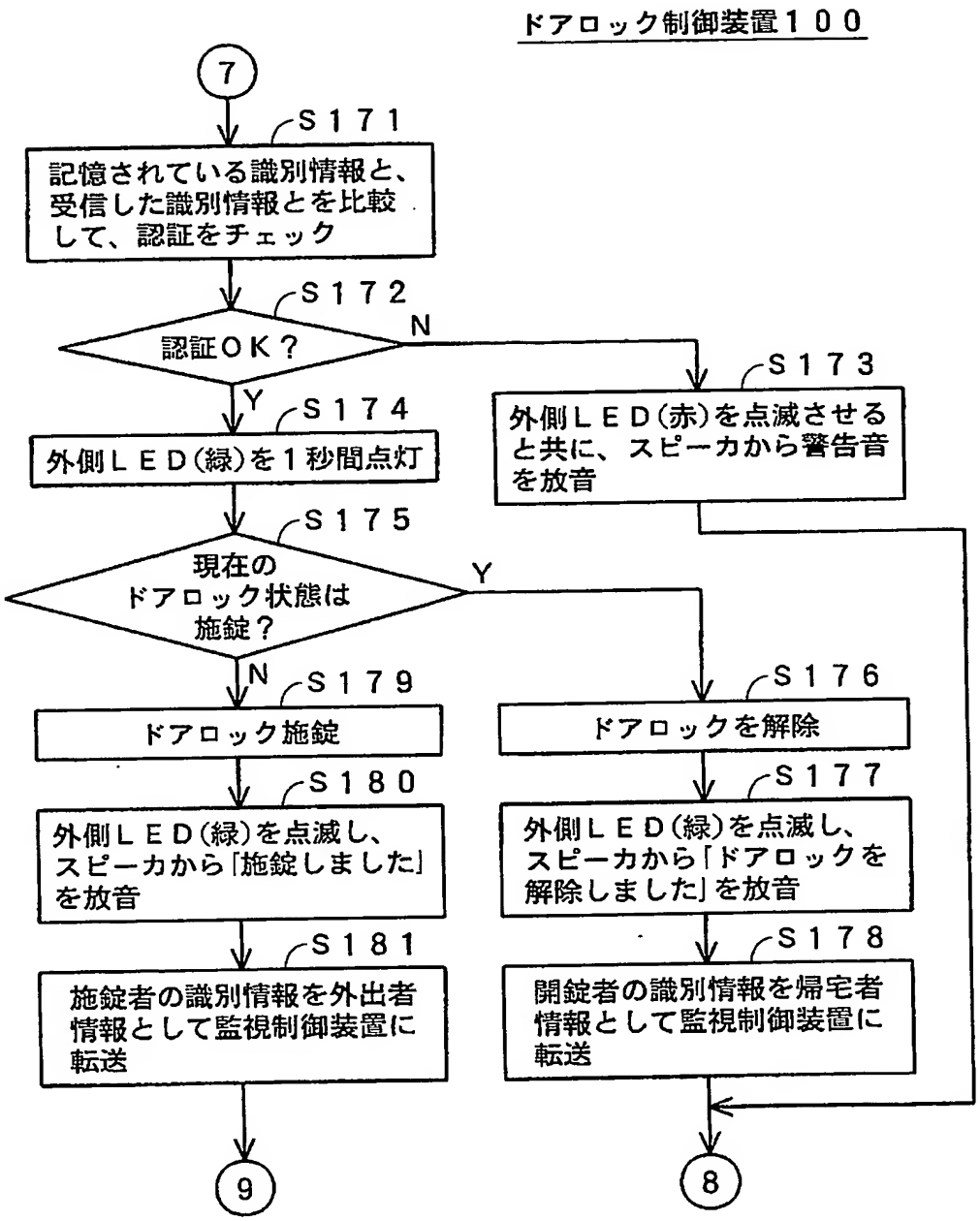
ドアロック制御装置１００



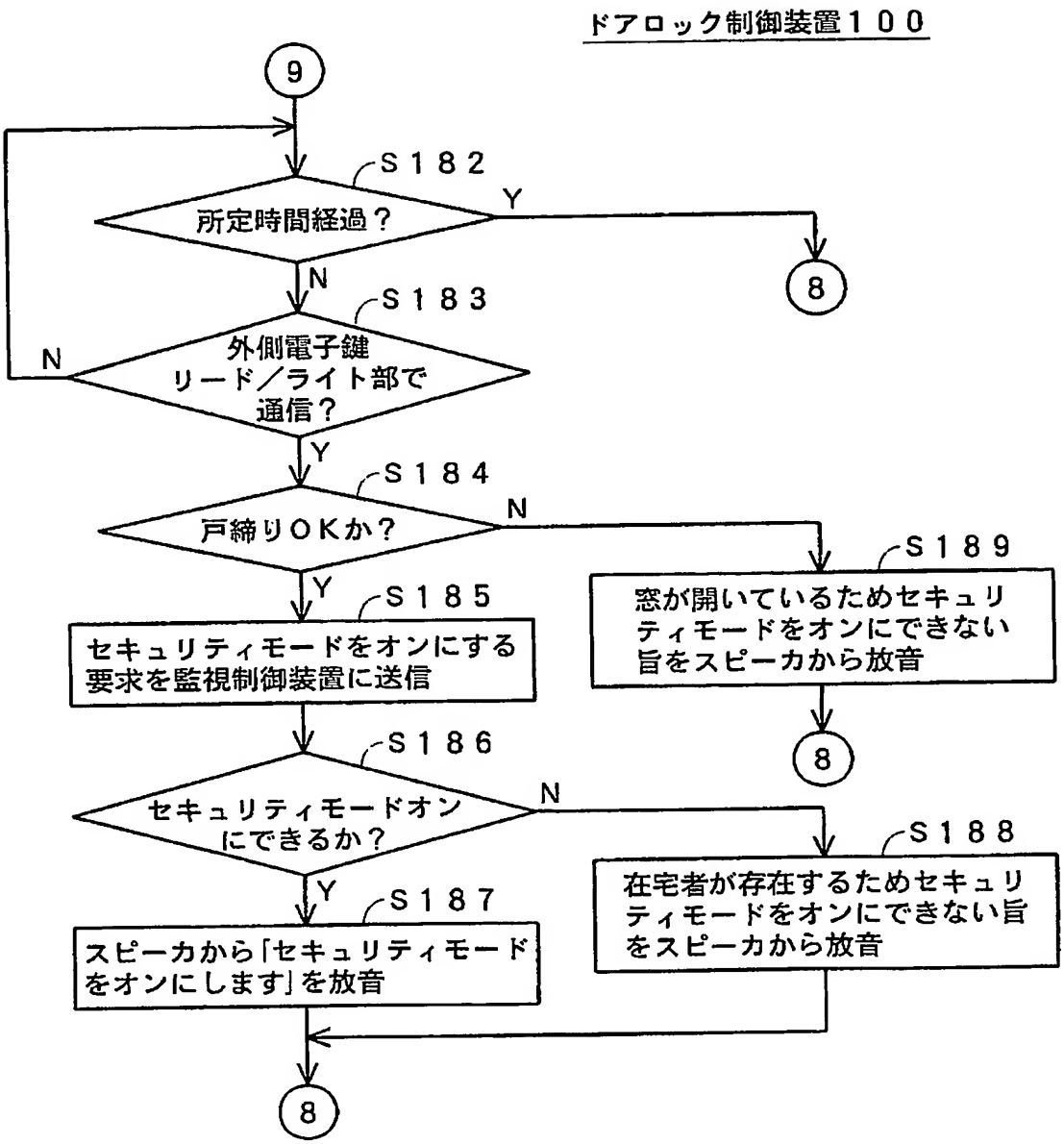
【図２７】


ドアロック制御装置１００
逐次ロックモード
8
S１５１
電子鍵装置と通信？
N
Y
S１５２
識別情報の取り込み
S１５３
内側ｏｒ外側？
外側
7
内側
S１５４
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１５５
認証ＯＫ？
N
S１５６
内側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
Y
S１５７
内側ＬＥＤ(緑)を１秒間点灯
S１５８
現在のドアロック状態は施錠？
Y
N
S１５９
ドアロック施錠
S１６０
内側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
S１６１
施錠者の識別情報を在宅者情報として監視制御装置に転送
S１６２
ドアロックを解除
S１６３
内側ＬＥＤ(緑)を点滅し、スピーカから「ドアロックを解除しました」を放音
S１６４
開錠者の識別情報を外出者情報として監視制御装置に転送

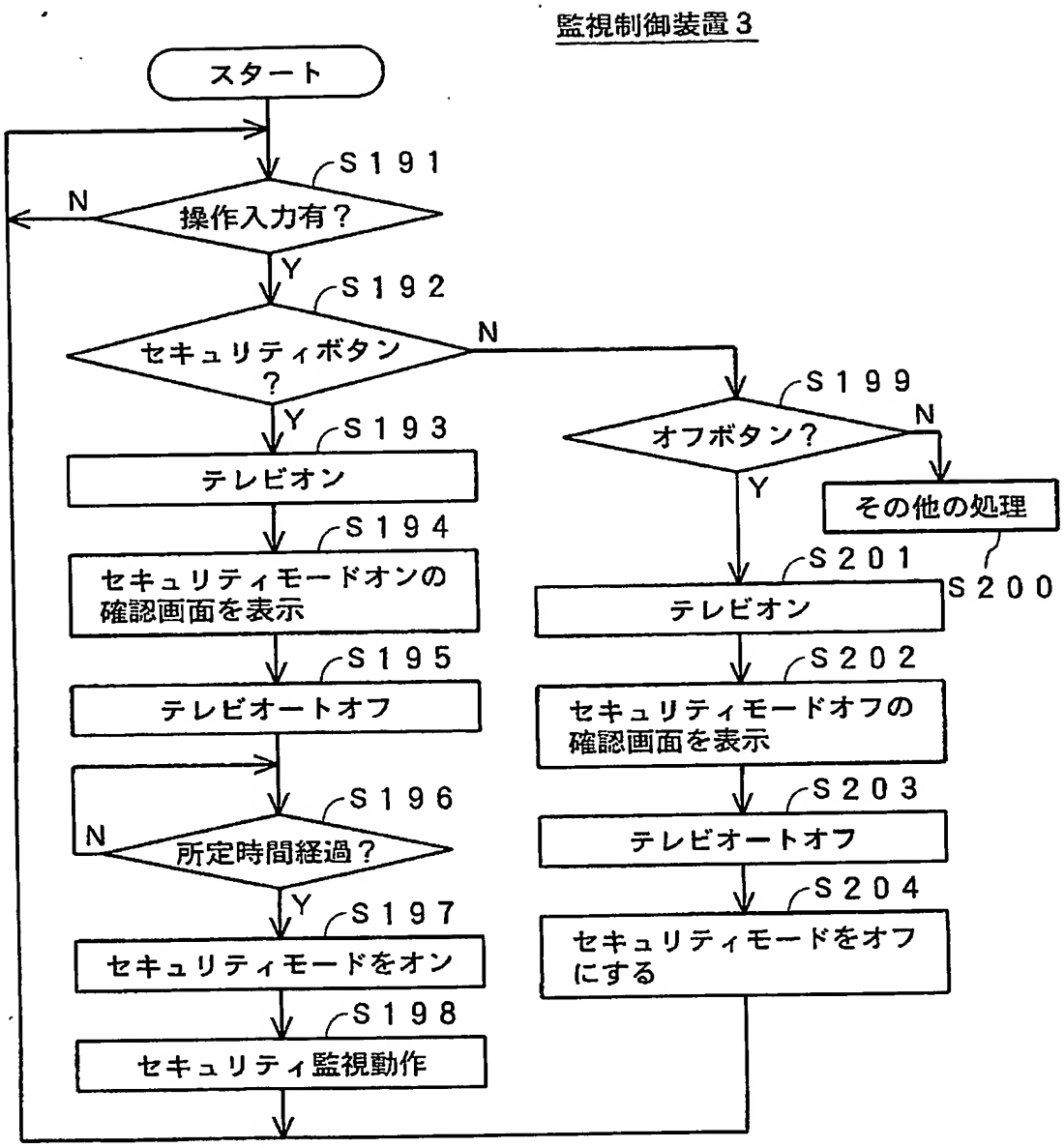
【図２８】


ドアロック制御装置１００
7
S１７１
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１７２
認証ＯＫ？
N
Y
S１７３
外側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
S１７４
外側ＬＥＤ(緑)を１秒間点灯
S１７５
現在のドアロック状態は施錠？
Y
N
S１７６
ドアロックを解除
S１７７
外側ＬＥＤ(緑)を点滅し、スピーカから「ドアロックを解除しました」を放音
S１７８
開錠者の識別情報を帰宅者情報として監視制御装置に転送
S１７９
ドアロック施錠
S１８０
外側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
S１８１
施錠者の識別情報を外出者情報として監視制御装置に転送
9
8

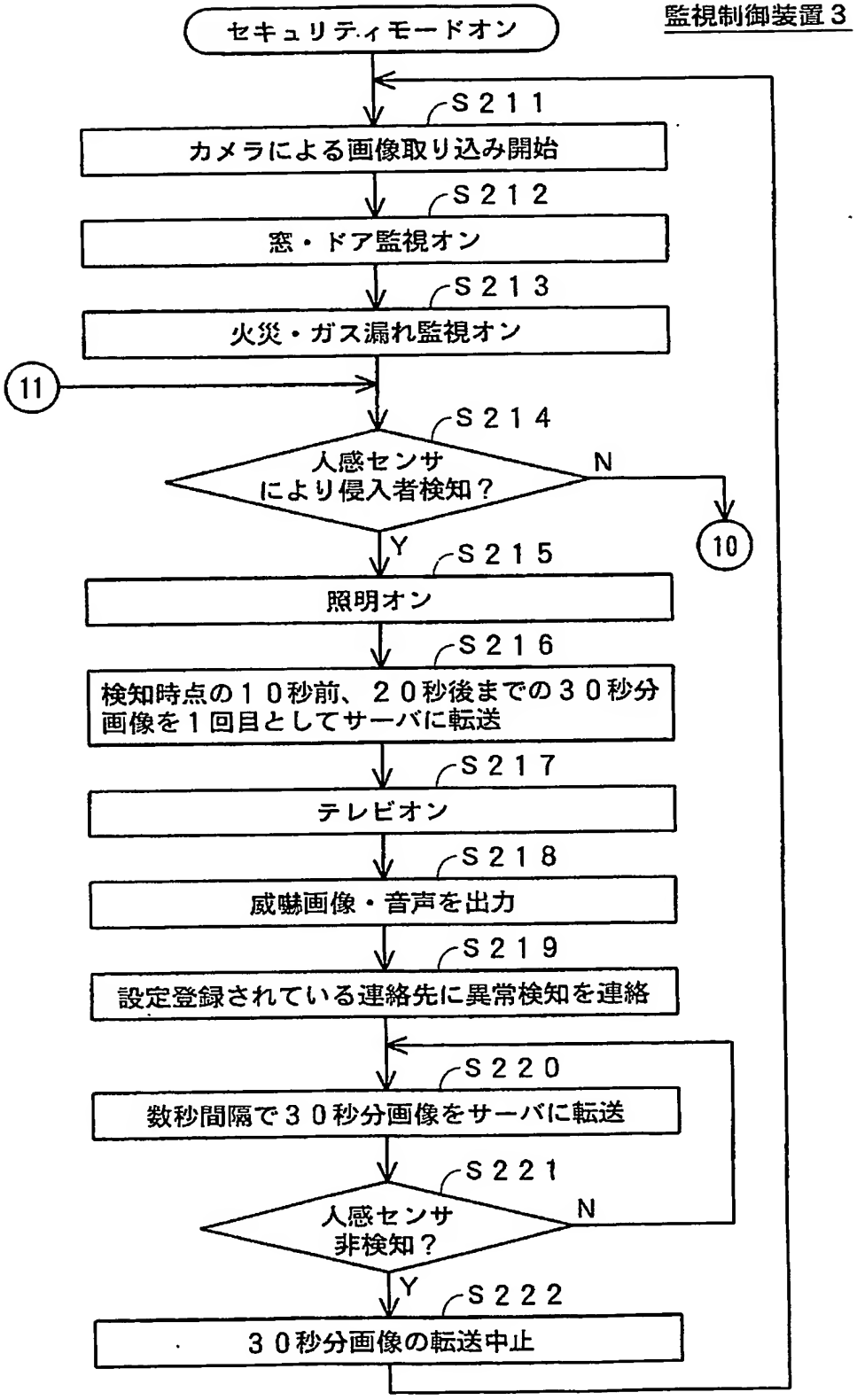
【図２９】


ドアロック制御装置１００
9
S１８２
所定時間経過？
Y
N
8
S１８３
外側電子鍵
リード／ライト部で
通信？
N
Y
S１８４
戸締りＯＫか？
N
Y
S１８９
窓が開いているためセキュリティモードをオンにできない旨をスピーカから放音
8
S１８５
セキュリティモードをオンにする要求を監視制御装置に送信
S１８６
セキュリティモードオンにできるか？
N
Y
S１８８
在宅者が存在するためセキュリティモードをオンにできない旨をスピーカから放音
S１８７
スピーカから「セキュリティモードをオンにします」を放音
8

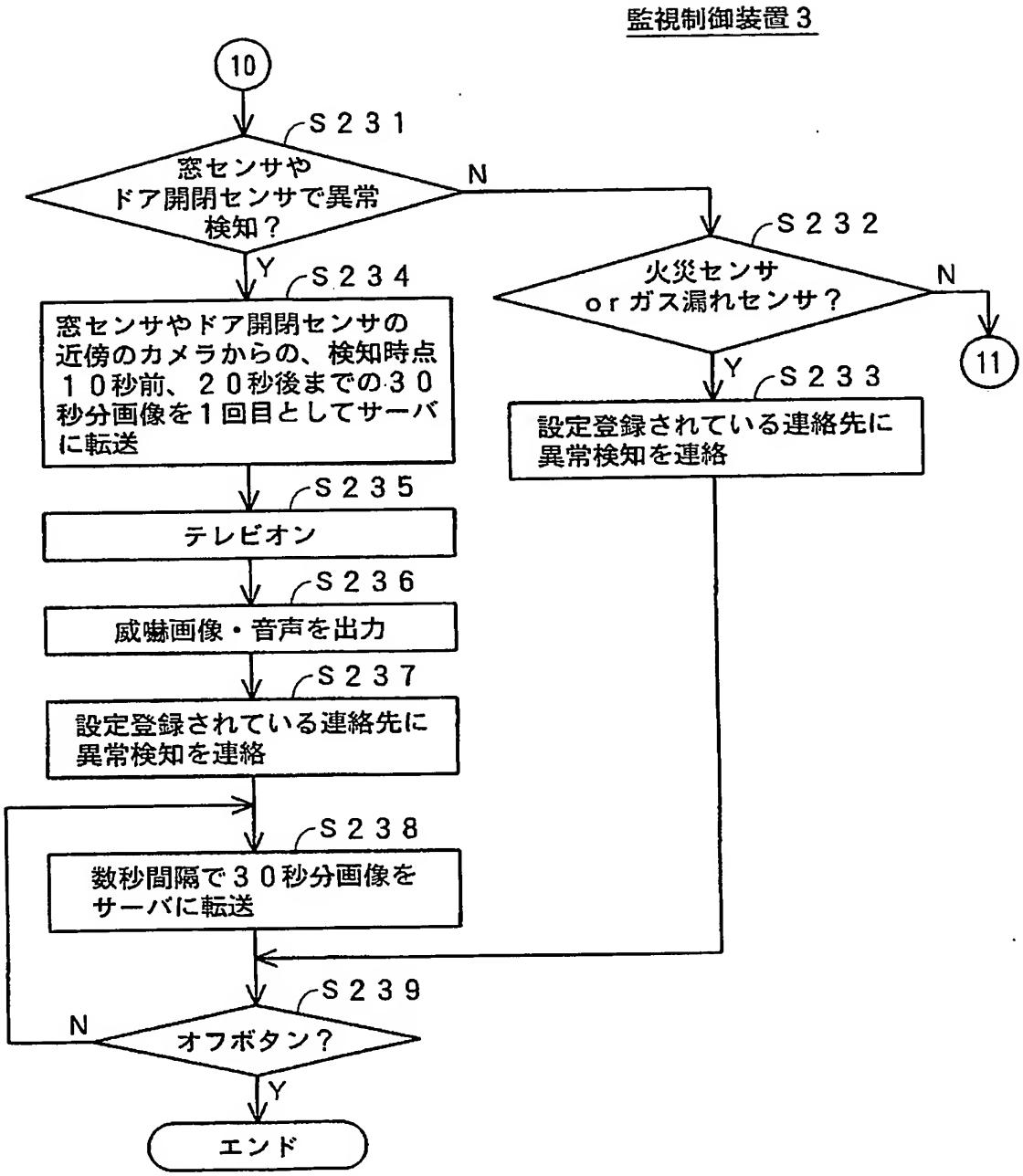
【図３０】


監視制御装置３
スタート
S１９１
操作入力有？
N
Y
S１９２
セキュリティボタン？
N
Y
S１９３
テレビオン
S１９４
セキュリティモードオンの確認画面を表示
S１９５
テレビオートオフ
S１９６
所定時間経過？
N
Y
S１９７
セキュリティモードをオン
S１９８
セキュリティ監視動作
S１９９
オフボタン？
N
Y
その他の処理
S２００
S２０１
テレビオン
S２０２
セキュリティモードオフの確認画面を表示
S２０３
テレビオートオフ
S２０４
セキュリティモードをオフにする

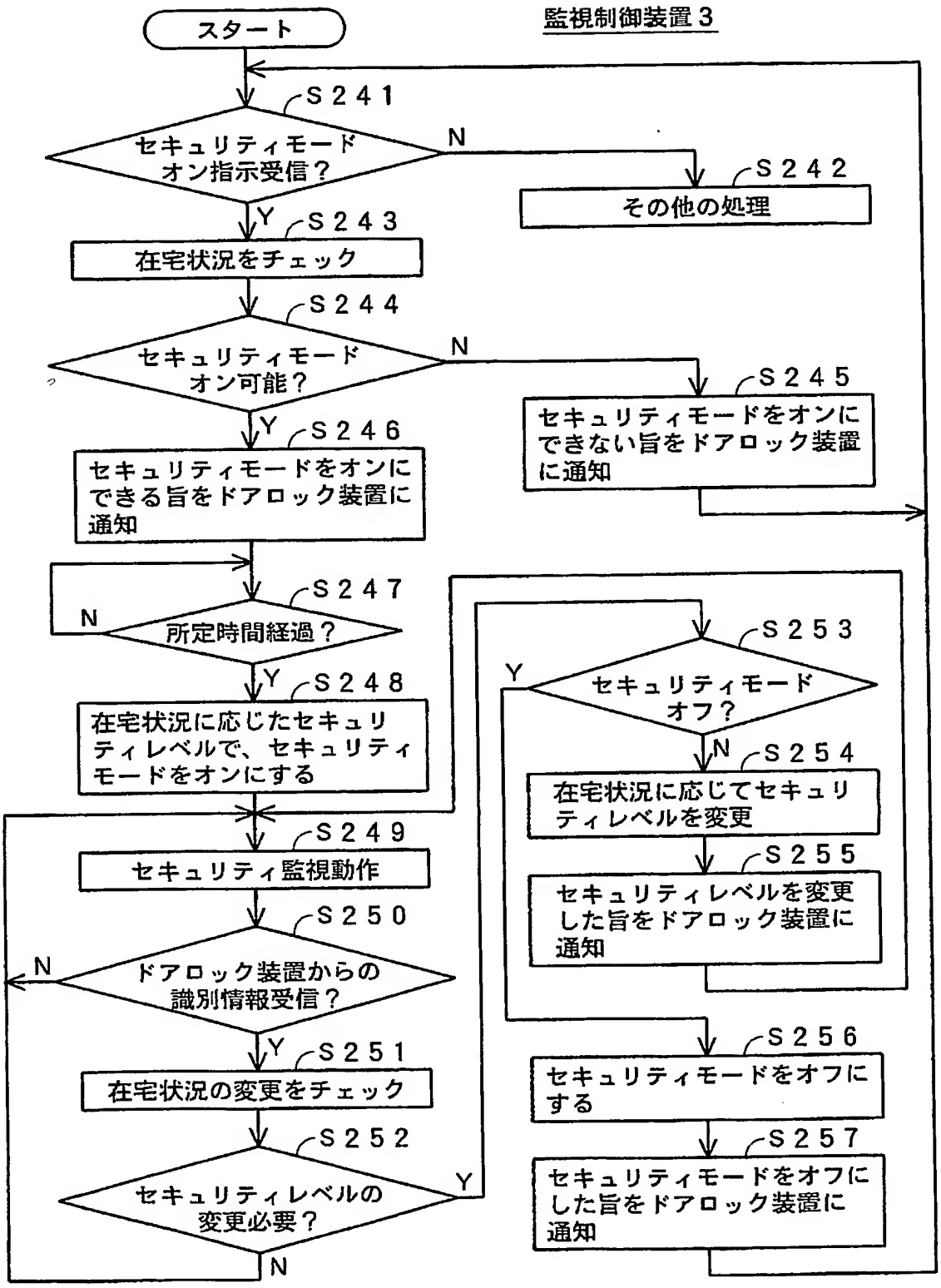
【図３１】


監視制御装置３
セキュリティモードオン
S２１１
カメラによる画像取り込み開始
S２１２
窓・ドア監視オン
S２１３
火災・ガス漏れ監視オン
11
S２１４
人感センサ
により侵入者検知？
N
10
Y
S２１５
照明オン
S２１６
検知時点の１０秒前、２０秒後までの３０秒分
画像を１回目としてサーバに転送
S２１７
テレビオン
S２１８
威嚇画像・音声を出力
S２１９
設定登録されている連絡先に異常検知を連絡
S２２０
数秒間隔で３０秒分画像をサーバに転送
S２２１
人感センサ
非検知？
N
Y
S２２２
３０秒分画像の転送中止

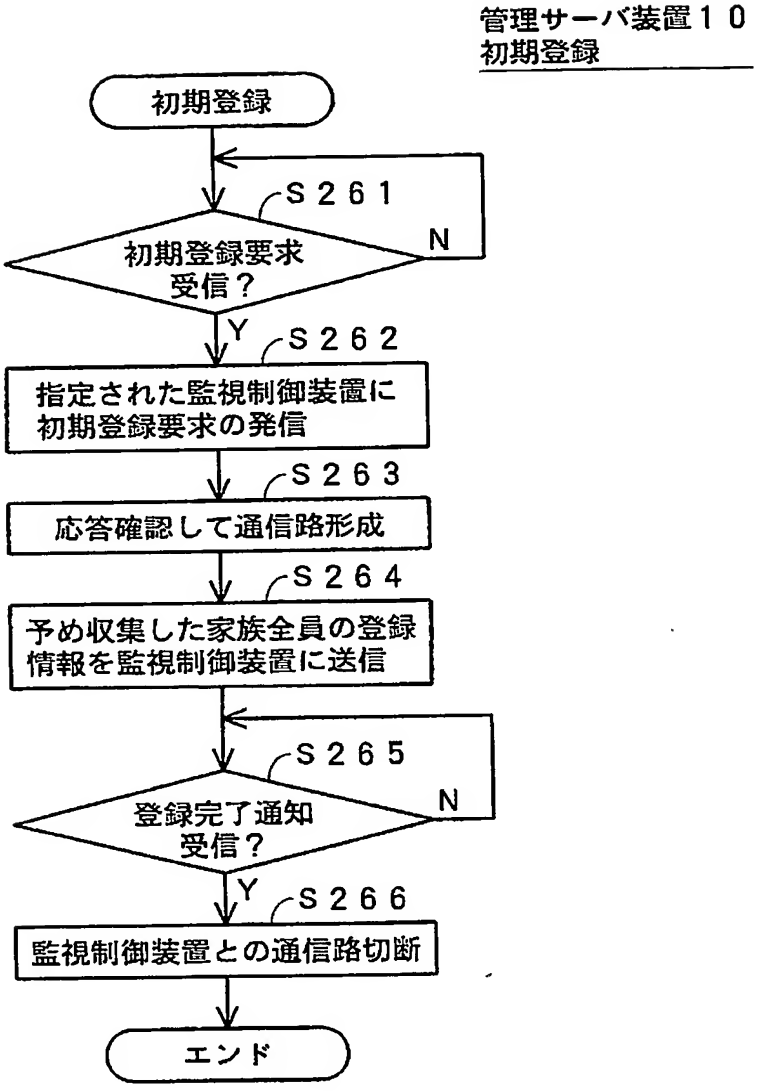
【図３２】


監視制御装置３
10
S２３１
窓センサや
ドア開閉センサで異常
検知？
N
Y
S２３２
火災センサ
ｏｒガス漏れセンサ？
N
Y
11
S２３３
設定登録されている連絡先に
異常検知を連絡
S２３４
窓センサやドア開閉センサの
近傍のカメラからの、検知時点
１０秒前、２０秒後までの３０
秒分画像を１回目としてサーバ
に転送
S２３５
テレビオン
S２３６
威嚇画像・音声を出力
S２３７
設定登録されている連絡先に
異常検知を連絡
S２３８
数秒間隔で３０秒分画像を
サーバに転送
S２３９
N
オフボタン？
Y
エンド

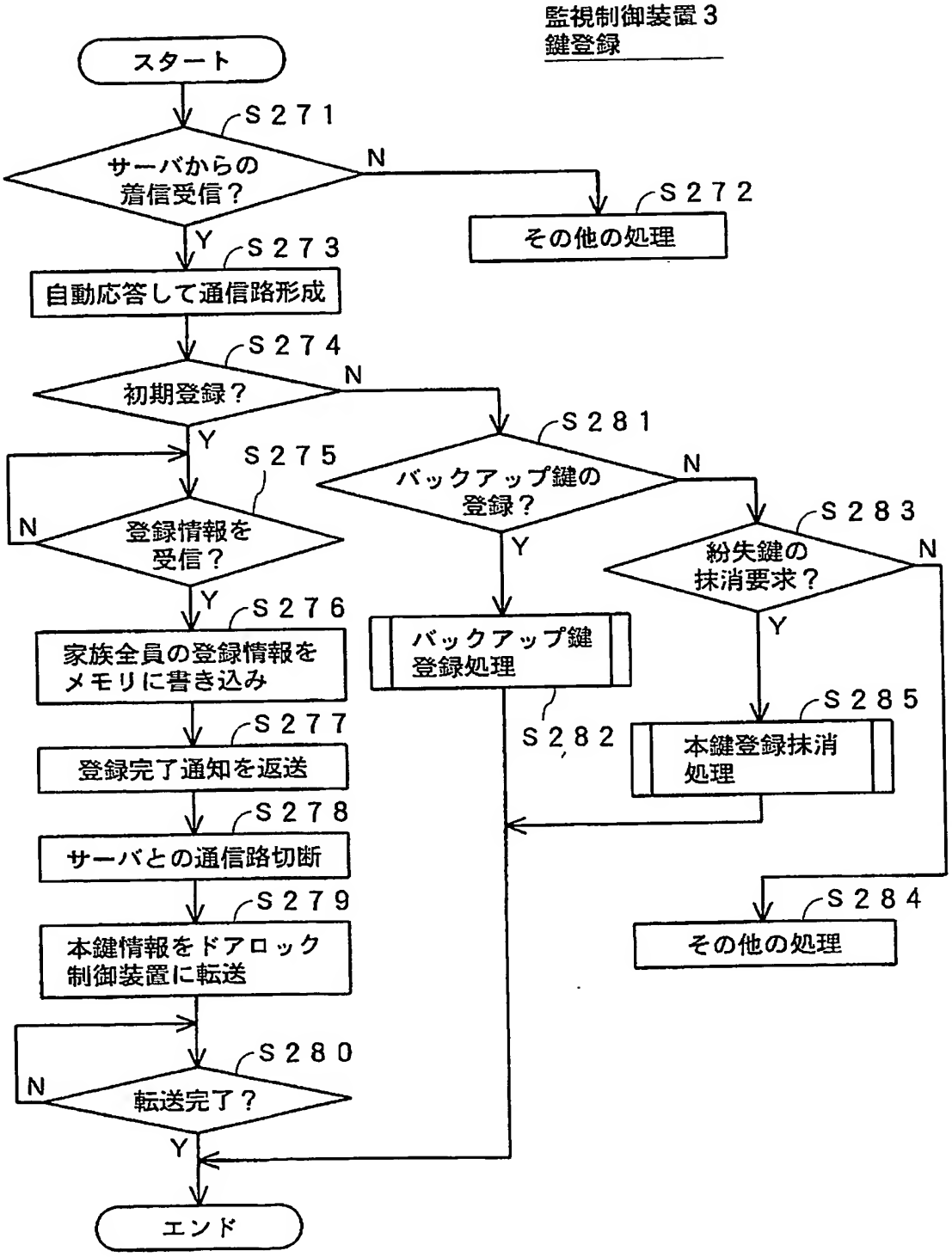
【図３３】


監視制御装置３
スタート
S２４１
セキュリティモード
オン指示受信？
N
S２４２
その他の処理
Y
S２４３
在宅状況をチェック
S２４４
セキュリティモード
オン可能？
N
S２４５
セキュリティモードをオンに
できない旨をドアロック装置
に通知
Y
S２４６
セキュリティモードをオンに
できる旨をドアロック装置に
通知
S２４７
N
所定時間経過？
Y
S２４８
在宅状況に応じたセキュリ
ティレベルで、セキュリティ
モードをオンにする
S２４９
セキュリティ監視動作
S２５０
N
ドアロック装置からの
識別情報受信？
Y
S２５１
在宅状況の変更をチェック
S２５２
セキュリティレベルの
変更必要？
Y
N
S２５３
Y
セキュリティモード
オフ？
N
S２５４
在宅状況に応じてセキュリ
ティレベルを変更
S２５５
セキュリティレベルを変更
した旨をドアロック装置に
通知
S２５６
セキュリティモードをオフに
する
S２５７
セキュリティモードをオフに
した旨をドアロック装置に
通知

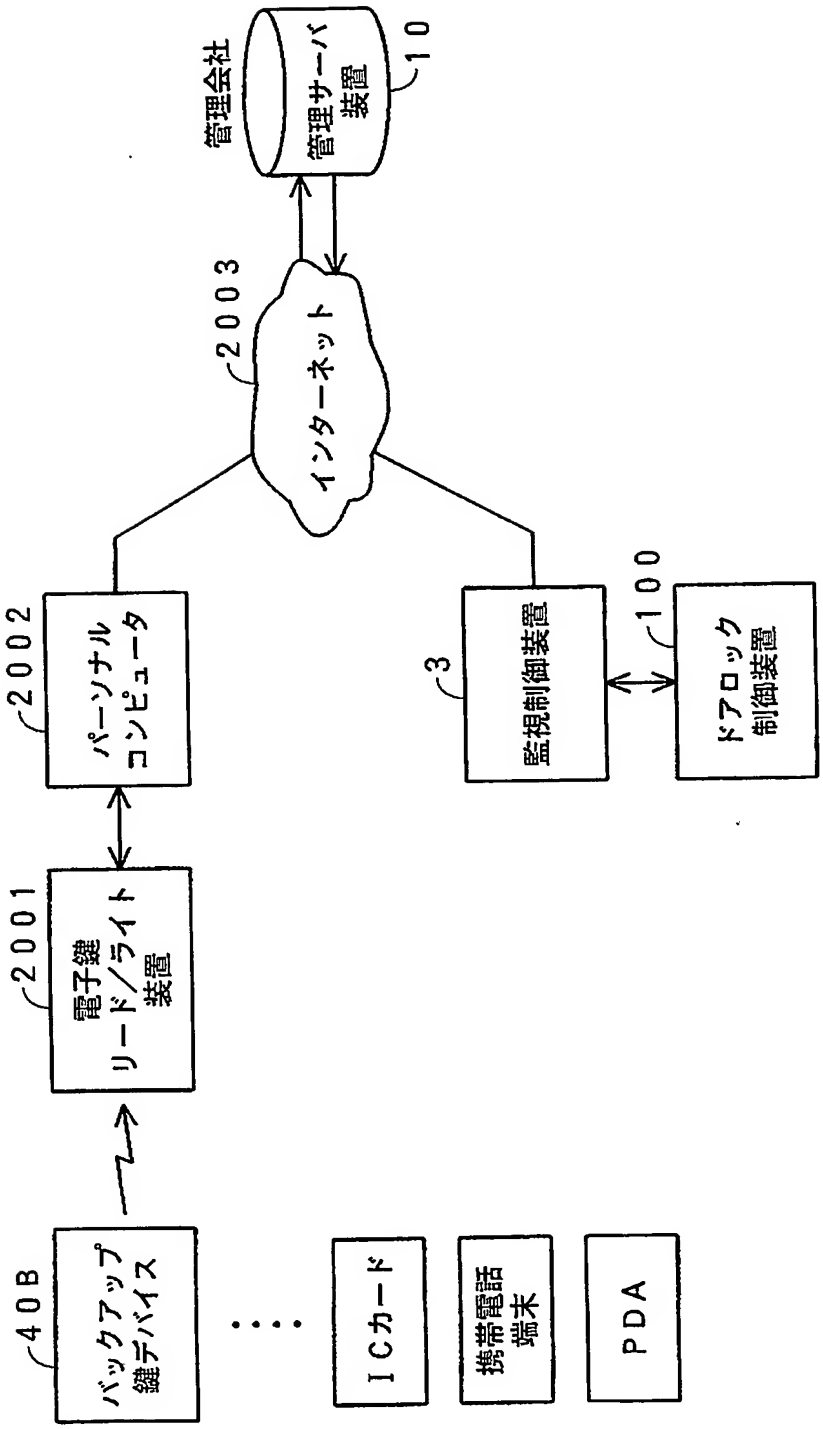
【図３４】


管理サーバ装置１０
初期登録
初期登録
Ｓ２６１
初期登録要求
受信？
N
Y
Ｓ２６２
指定された監視制御装置に
初期登録要求の発信
Ｓ２６３
応答確認して通信路形成
Ｓ２６４
予め収集した家族全員の登録
情報を監視制御装置に送信
Ｓ２６５
登録完了通知
受信？
N
Y
Ｓ２６６
監視制御装置との通信路切断
エンド

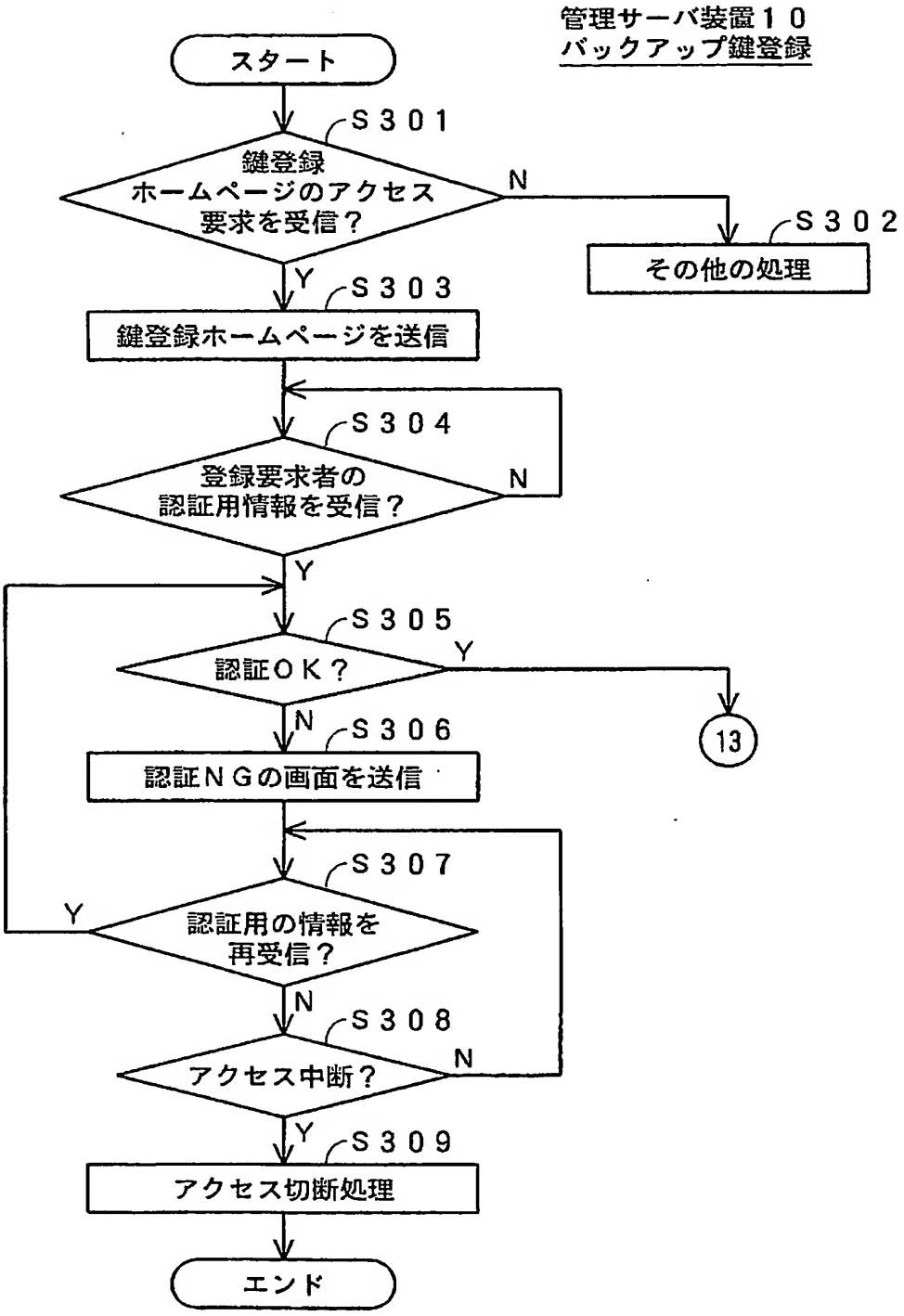
【図３５】


監視制御装置３
鍵登録
スタート
S２７１
サーバからの着信受信？
N
S２７２
その他の処理
Y
S２７３
自動応答して通信路形成
S２７４
初期登録？
N
Y
S２８１
バックアップ鍵の登録？
N
S２８３
紛失鍵の抹消要求？
N
Y
S２７５
N
登録情報を受信？
Y
S２７６
家族全員の登録情報をメモリに書き込み
S２７７
登録完了通知を返送
S２７８
サーバとの通信路切断
S２７９
本鍵情報をドアロック制御装置に転送
S２８０
N
転送完了？
Y
エンド
Y
バックアップ鍵登録処理
S２８２
S２８５
本鍵登録抹消処理
S２８４
その他の処理

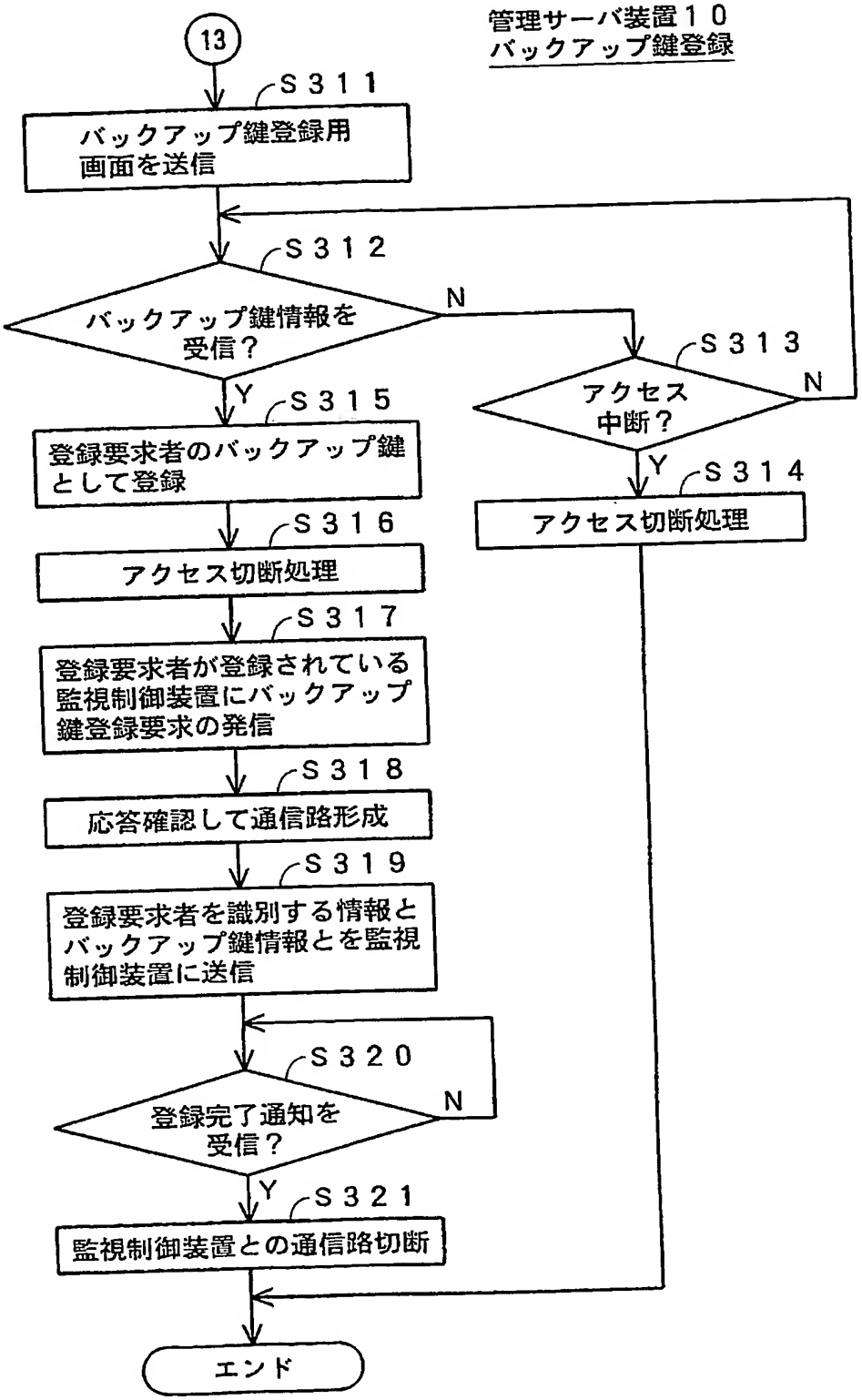
【図３６】


管理会社
管理サーバ装置
10
2003
インターネット
2002
パーソナルコンピュータ
3
監視制御装置
100
ドアロック制御装置
2001
電子鍵リード／ライト装置
40B
バックアップ鍵デバイス
ICカード
携帯電話端末
PDA

【図３７】

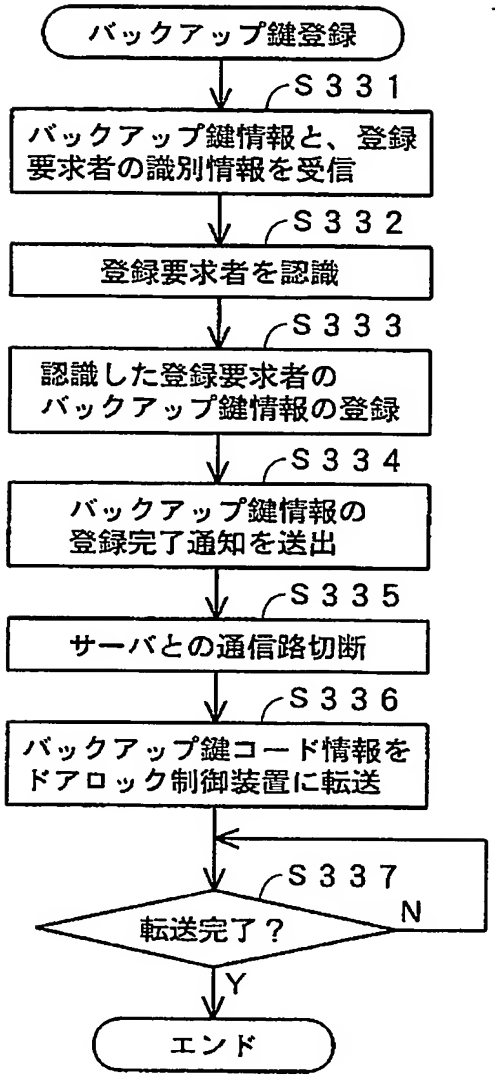

管理サーバ装置１０
バックアップ鍵登録
スタート
Ｓ３０１
鍵登録
ホームページのアクセス
要求を受信？
N
Ｓ３０２
その他の処理
Y
Ｓ３０３
鍵登録ホームページを送信
Ｓ３０４
登録要求者の
認証用情報を受信？
N
Y
Ｓ３０５
認証ＯＫ？
Y
13
N
Ｓ３０６
認証ＮＧの画面を送信
Ｓ３０７
Y
認証用の情報を
再受信？
N
Ｓ３０８
アクセス中断？
N
Y
Ｓ３０９
アクセス切断処理
エンド

【図３８】

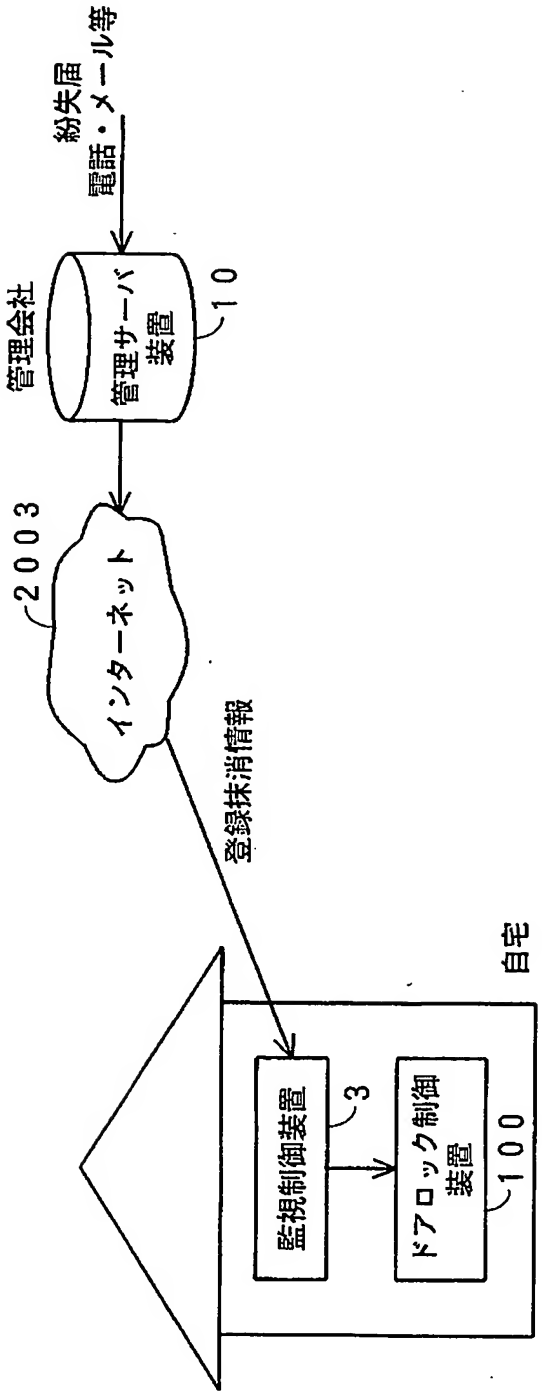

管理サーバ装置１０
バックアップ鍵登録
13
S３１１
バックアップ鍵登録用画面を送信
S３１２
バックアップ鍵情報を受信？
N
Y
S３１３
アクセス中断？
N
Y
S３１４
アクセス切断処理
S３１５
登録要求者のバックアップ鍵として登録
S３１６
アクセス切断処理
S３１７
登録要求者が登録されている監視制御装置にバックアップ鍵登録要求の発信
S３１８
応答確認して通信路形成
S３１９
登録要求者を識別する情報とバックアップ鍵情報とを監視制御装置に送信
S３２０
登録完了通知を受信？
N
Y
S３２１
監視制御装置との通信路切断
エンド

【図３９】

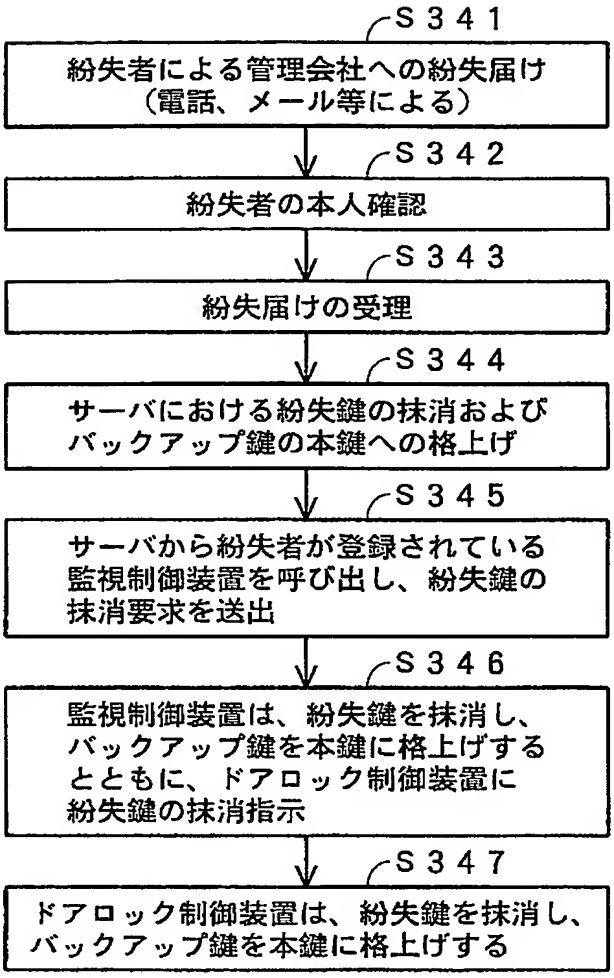
監視制御装置３
バックアップ鍵登録



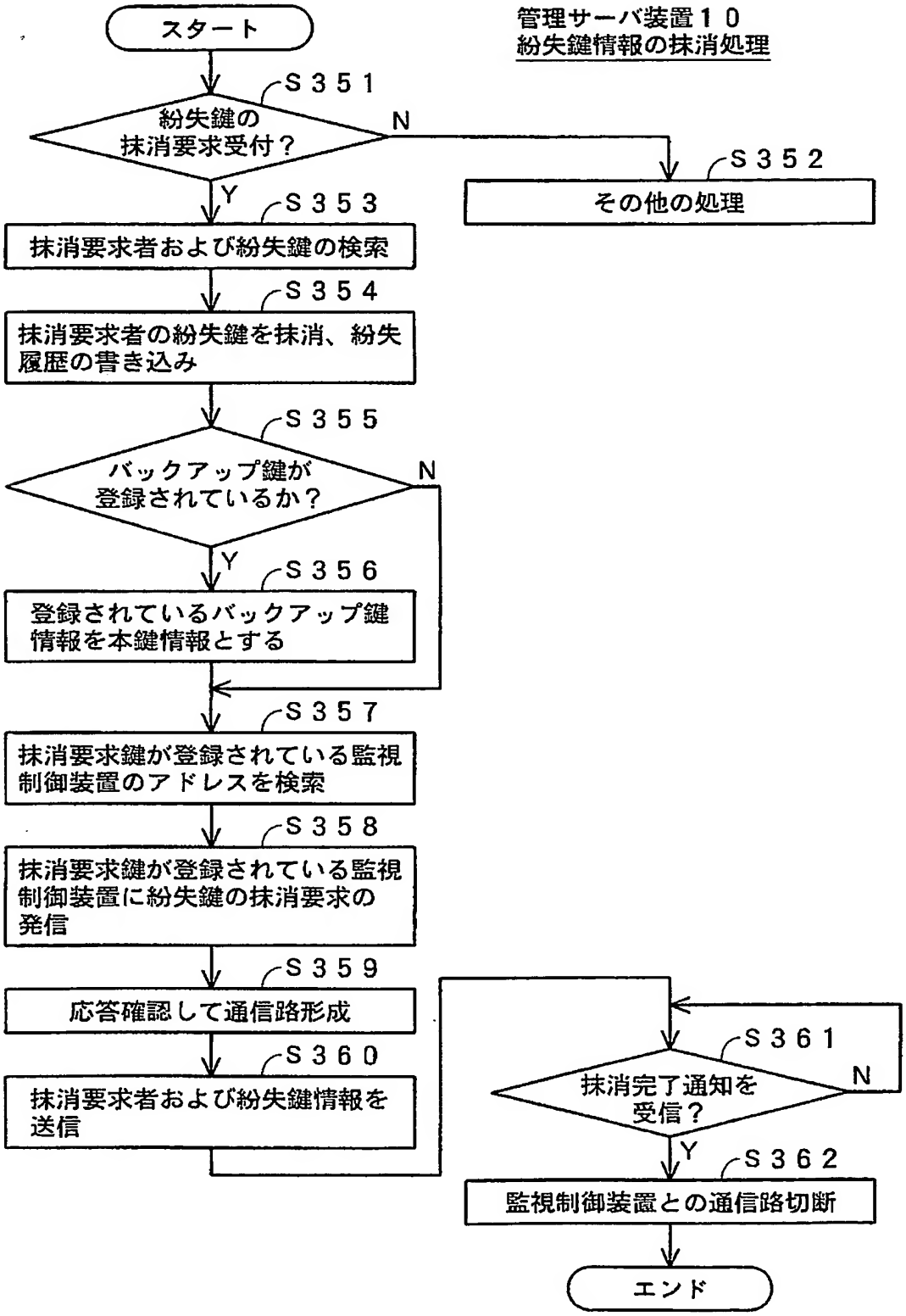
【図４０】


紛失届
電話・メール等
管理会社
管理サーバ
装置
10
2003
インターネット
登録抹消情報
自宅
監視制御装置
3
ドアロック制御
装置
100

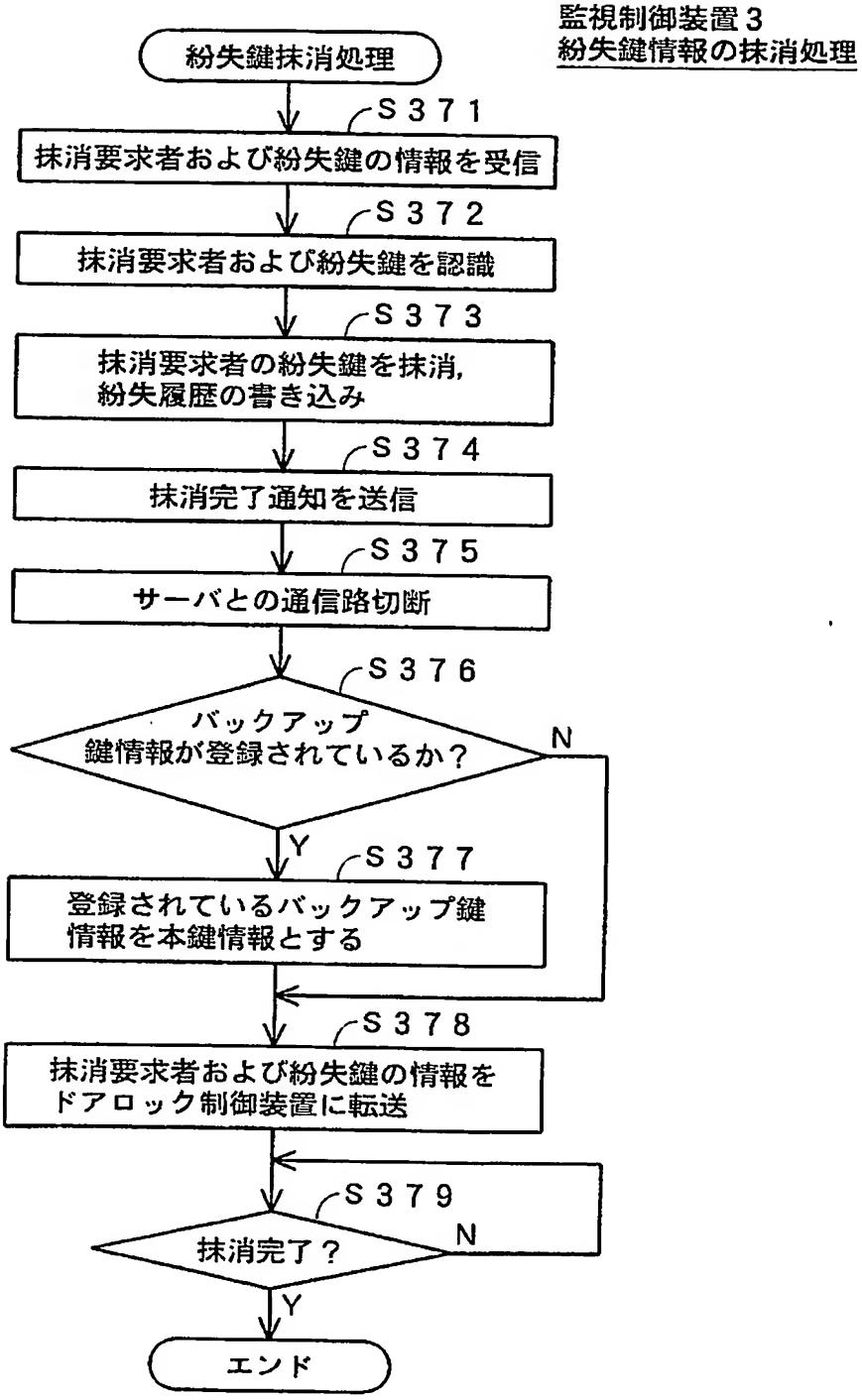
【図４１】


紛失鍵の抹消手順
Ｓ３４１
紛失者による管理会社への紛失届け
（電話、メール等による）
Ｓ３４２
紛失者の本人確認
Ｓ３４３
紛失届けの受理
Ｓ３４４
サーバにおける紛失鍵の抹消および
バックアップ鍵の本鍵への格上げ
Ｓ３４５
サーバから紛失者が登録されている
監視制御装置を呼び出し、紛失鍵の
抹消要求を送出
Ｓ３４６
監視制御装置は、紛失鍵を抹消し、
バックアップ鍵を本鍵に格上げする
とともに、ドアロック制御装置に
紛失鍵の抹消指示
Ｓ３４７
ドアロック制御装置は、紛失鍵を抹消し、
バックアップ鍵を本鍵に格上げする

【図４２】

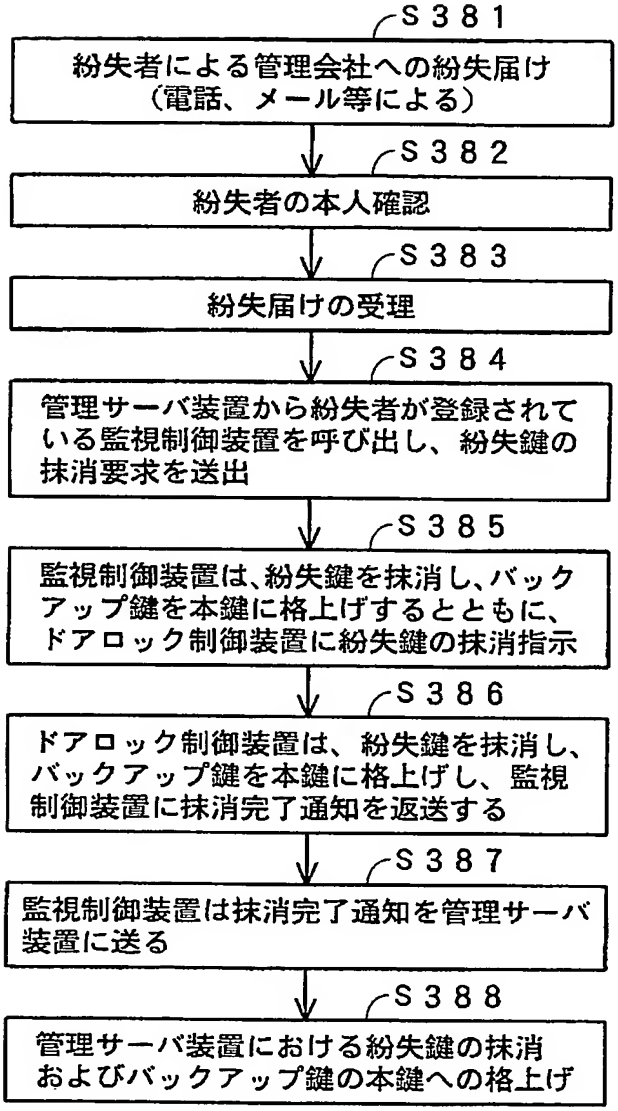

スタート
管理サーバ装置１０
紛失鍵情報の抹消処理
Ｓ３５１
紛失鍵の
抹消要求受付？
N
Ｓ３５２
その他の処理
Y
Ｓ３５３
抹消要求者および紛失鍵の検索
Ｓ３５４
抹消要求者の紛失鍵を抹消、紛失
履歴の書き込み
Ｓ３５５
バックアップ鍵が
登録されているか？
N
Y
Ｓ３５６
登録されているバックアップ鍵
情報を本鍵情報とする
Ｓ３５７
抹消要求鍵が登録されている監視
制御装置のアドレスを検索
Ｓ３５８
抹消要求鍵が登録されている監視
制御装置に紛失鍵の抹消要求の
発信
Ｓ３５９
応答確認して通信路形成
Ｓ３６０
抹消要求者および紛失鍵情報を
送信
Ｓ３６１
抹消完了通知を
受信？
N
Y
Ｓ３６２
監視制御装置との通信路切断
エンド

【図４３】

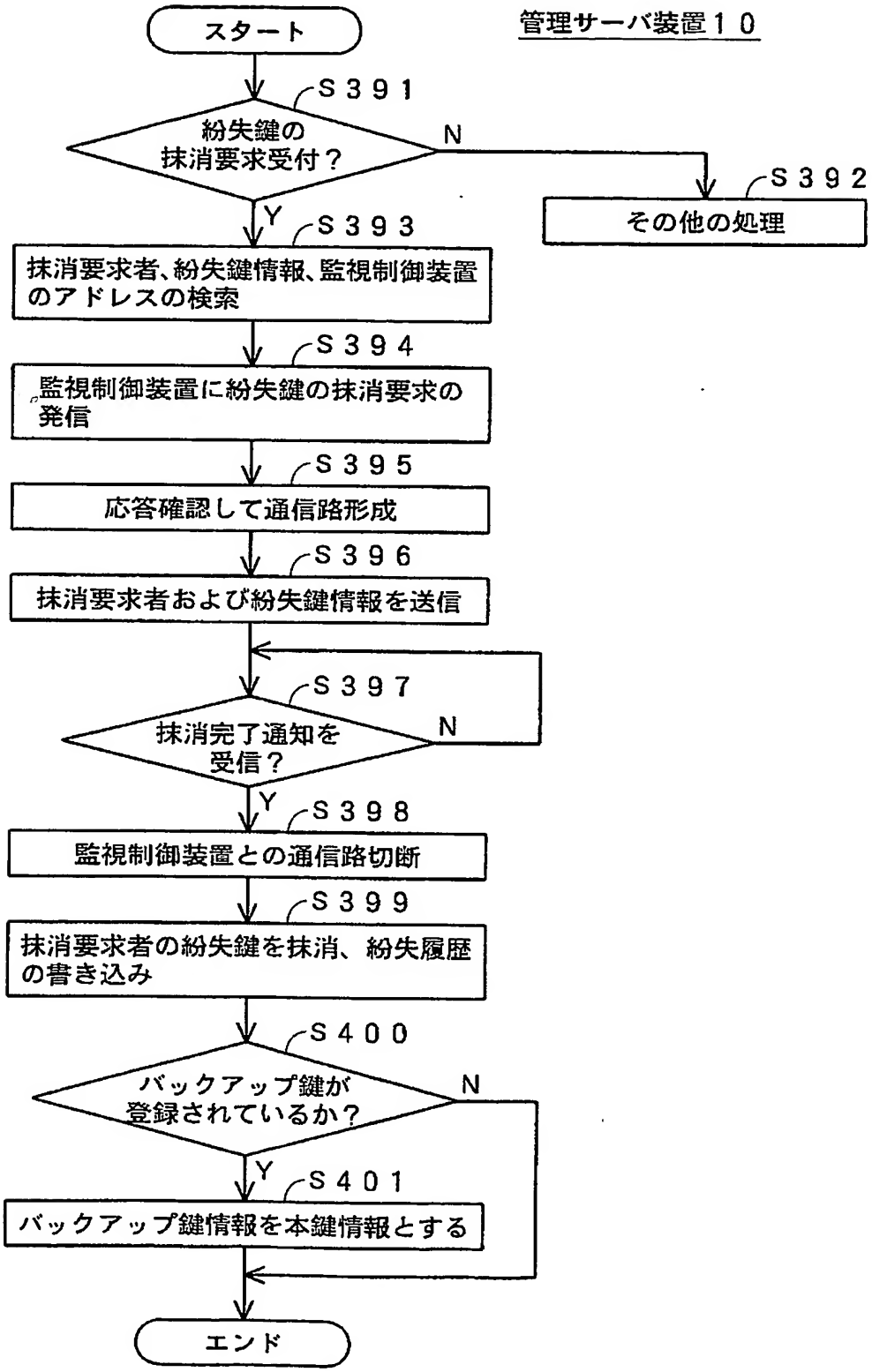

監視制御装置３
紛失鍵情報の抹消処理
紛失鍵抹消処理
Ｓ３７１
抹消要求者および紛失鍵の情報を受信
Ｓ３７２
抹消要求者および紛失鍵を認識
Ｓ３７３
抹消要求者の紛失鍵を抹消，
紛失履歴の書き込み
Ｓ３７４
抹消完了通知を送信
Ｓ３７５
サーバとの通信路切断
Ｓ３７６
バックアップ
鍵情報が登録されているか？
N
Y
Ｓ３７７
登録されているバックアップ鍵
情報を本鍵情報とする
Ｓ３７８
抹消要求者および紛失鍵の情報を
ドアロック制御装置に転送
Ｓ３７９
抹消完了？
N
Y
エンド

【図４４】

紛失鍵の抹消手順



【図４５】


管理サーバ装置１０
スタート
S３９１
紛失鍵の抹消要求受付？
N
S３９２
その他の処理
Y
S３９３
抹消要求者、紛失鍵情報、監視制御装置のアドレスの検索
S３９４
監視制御装置に紛失鍵の抹消要求の発信
S３９５
応答確認して通信路形成
S３９６
抹消要求者および紛失鍵情報を送信
S３９７
抹消完了通知を受信？
N
Y
S３９８
監視制御装置との通信路切断
S３９９
抹消要求者の紛失鍵を抹消、紛失履歴の書き込み
S４００
バックアップ鍵が登録されているか？
N
Y
S４０１
バックアップ鍵情報を本鍵情報とする
エンド

【書類名】　　要約書

【要約】

【課題】　紛失しても、容易に悪意の紛失鍵の拾得者に対抗することができる電子鍵装置を提供する。

【解決手段】　生体情報を取得する生体情報取得手段４１と、生体情報が記憶されている生体情報記憶部４０８と、電子鍵情報が記憶されている電子鍵情報記憶部４０５と、電子鍵情報を外部に送信する機能を備える通信手段４２と、生体情報取得手段４１で取得された生体情報と、生体情報記憶部４０８に記憶されている生体情報とを比較する比較手段と、比較手段での比較結果に基づいて、電子鍵情報記憶部の電子鍵情報の通信手段４２を通じた送出を制御する制御手段４０１とを備える。

【選択図】　　図５

特願２００２－２９８３０９

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社